Tackling DNS abuse in the Caribbean

The DNS Observatory

Shernon Osepa

Consultant / Advisor CTU

shernon.osepa@ctu.int

Shaping Caribbean ICT Development

DNS abuse definition

is composed of five/six* broad categories of harmful activity insofar as they intersect with the DNS:

(ICANN Registrar / gTLDs Registries Stakeholder groups / Internet & Jurisdiction Policy Network)

Categories of DNS abuses

Technical:

- Malware;
- Botnets;
- Phishing;
- Pharming;
- Spam;
- Fast-flux hosting.

Categories of DNS abuses - 2

Website content:

- Child abuse material;
- Controlled substances and Regulated goods (illegal drugs, stolen goods, illegal firearms, etc.);
- Violent extremist content;
- Hate speech;
- Intellectual property related.

Some Newspapers' Headlines

JAMAICA OBSERVER

ePaper

Home News Business Olympics Sports Entertainment Lifestyle All Woman Obituaries Classifieds More

Jamaica suffered 43 million cyber attack attempts in 2023 — Fortinet

BUSINESS

Caribbean faced 144 million cyberattack attempts in 6 months

NEWSDAY REPORTER THURSDAY 9 FEBRUARY 2023

Trinidad's state telecoms company hit by cyberattack

Costa Rica Declares State of Emergency Under Sustained Conti Cyberattacks

Conti's ransomware attack cripples Costa Rica's Treasury, sparking the US to offer a $15M bounty on the group.

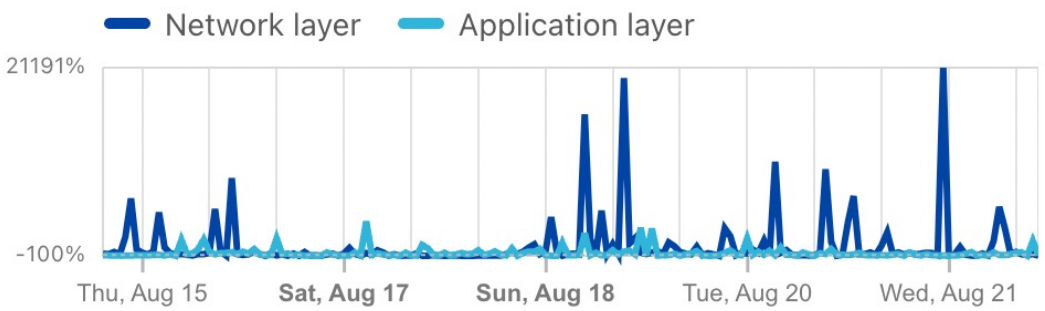
Shaping Caribbean ICT Development

Guyana is not immune

Security & Attacks in Guyana ✕ ⌄ Last 7 days

Attack volume

Relative change from previous period



UDP **99.99%**

WAF **85%**

TCP **0.01%**

DDoS **14%**

Top source ASes of application layer attacks

	ASN	Percentage
1	AS264694 - EGOVERNMENT UNIT	68.8%
2	AS19863 - Guyana Telephone & Telegraph Co.	17.8%
3	AS52253 - E-Networks Inc.	9.6%
4	AS52433 - U Mobile Cellular Inc.	3.3%
5	AS13335 - CLOUDFLARENET	0.3%

Shaping Caribbean ICT Development

What can we do about it?

- **Stakeholders**
  - Governments
  - Law enforcement entities
  - Business community
  - Academia
  - Civil society

- **Caribbean Telecommunications Union**
  - A holistic approach (policy, capacity building, collaboration, enforcement).

A Caribbean DNS Observatory

A tool that can help you track changes in the use of the DNS system

following patterns and trends

- **Government portals**
- **ccTLDs**

Stakeholders

- ICANN's LACRALOs
- CTU
  - Coordination

Structure of the work and planning (2 phases)

- Define the goals
- Choose the data sources
- Tools selection
- Tools configuration
- Analyze the data

Questions?

References

- ICANN Registrar Stakeholder Group
- Cloudflare radar
  - https://radar.cloudflare.com/security-and-attacks/gy
- https://newsday.co.tt/2023/02/09/caribbean-faced-144-million-cyberattack-attempts-in-6-months/
- https://dl.acm.org/doi/10.1145/3355369.3355566
- https://www.domaintools.com/resources/blog/tracking-the-dns-stars-the-dns-observatory/

Thank You!

Shernon Osepa

Shernon.osepa@ctu.int

+599 9 520-9613