NCAP Discussion Group Weekly Meeting - 21 April 2021

Agenda:

- Welcome and roll call
- ICANN Board's questions regarding name collisions: Board Questions working documents [drive.google.com]
- AOB

Board Question #3 discussion cont.

The harm to existing users that may occur if Collision Strings were to be delegated, including harm due to end systems no longer receiving a negative response and additional potential harm if the delegated registry accidentally or purposely exploited subsequent queries from these end systems, and any other types of harm.

1. Anne's additions to Board Question #3 was added by Matt T:

Some distinct types of harm which can be identified at this stage include the following:
DEFINE THESE FOR THE BOARD AND THE COMMUNITY

- Reconnaissance/enumeration
- MitM attacks (Man in the Middle attacks may need subgroups)
- Internal document leakage
- Personal document leakage
- Malicious Code Injection
- Credential Theft

Discussion Notes on #3 continue:

- Matt: ensure there is a coherent thread through all the answers to Board Questions.
- We need to determine the consequences for what happens if collision happens:
- we can't list every type of harm possible. Instead find categories of harm and explain why it matters and give examples. Example: Interception maniipulation: disclosure of info and

- Tom Barrett: there is an underlying assumption here that the app generating traffic that would collide with an icann tld is occurring at the root. what about collisions that do not occur at the root but were introduce by ICANN adding a new TLD?

    - Answer: Collisions below tld levels are outside icann & ncap study remit.

Definition of Name Collision from when preparing for Study 1:
https://community.icann.org/display/NCAP/NCAP+Working+Documents?preview=/79437474/111387704/Definition%20of%20Name%20Collision%20and%20Scope%20of%20Work%20for%20the%20NCAP.pdf

Duplicate Name Space Discussion

- Tom: So does .CRYPTO fall into the same category of CORP/HOME/mail
    - ANSWER: No. Corp/home/mail are LEGACY (Microsoft fixed their issues a while ago but some systems hardcoded and couldn't be changed) and .Crypto was a choice to duplicate ICANN name space without permission. Crypto is a "squatter"

- Collisions are managed by registrations being first come, first serve and you can't have a duplicate registration.

- Tom: .crypto is a start-up in CA using blockchain so they've they've basically been showing their customer base, how to alter DNS either on their machine basically on a machine, so that it goes drone all from it DNS. it doesn't collide with anything today, because there is no ICANN "crypto" at the root and so there's no error traffic at the root because it's called right alternative DNS. the question is, what happens if ICANN then delegates crypto at the root to someone, and people using .cyrpto originally have their web browser change what DNS its using, these people are "harmed?".

  ANSWER: So the the direct answer to your question is that that's not within our scope. .crypto is violating the ICANN rules and ICANN should not make an exception for them as this is not fair to those who are going through the ICANN process.

- .web is another (old) example and they disappeared

- Need to acknowledge alternative roots, but we don't weigh the harm done to users of .crypto like we weigh harm done to users of other tlds. This is because .crypto defied

the ICANN Community's process but duplicated the same technology. So, .crypto needs to have a different solution: doesn't matter if you harm people on .crypto because they are there illegally. Other name collisions are due to error – people setting up internal networks and not realizing the harm. .cyrpto knew what would happen. Make sure you have a separate rule.

- MATT: BOARD QUESTION #9 may encompass this: *measures to protect against intentional or unintentional creation of situations, such as queries for undelegated strings, which might cause such strings to be placed in a Collision String category, and research into risk of possible negative effects, if any, of creation of such a collision string list.*

- .onion: IETF designated it as special use name (.onion, while ICANNers didn't like it, was done according to the process set forth in the IETF/ICANN MoU) and that means that ICANN will consider if there are other name spaces (lists of names) that it might want to consider reserved like .onion. should the IETF special use domains list be reserved in future ICANN gTLD rounds?

- There was concern about .onion setting a precedent for squatters but using special use list. (IETF said there was significant security issue with .onion) . IETF should issue this as a statement then so we have documentation, but the NCAP Discussion group received some evidence that as IETF turned away a pipeline of other names up for discussion to be put on the special use name, and decided to only accept .onion because of extra security issues, that IETF recognizes .onion as a one-off.

- Study 2 should consider a recommendation asking for the IETF to make a statement in writing regarding special use names and if they will have a process ot add names in the future or not. 12:42PM

- MOU IETF & ICANN & ISOC, subpro looked at this and recommended no changes to .onion

- AT 12:46 Jeff brought up letter from Goran; wants to get more recent status so we don't make unneeded recommendations:

  Letter from Goran Marby to the IETF in October 2020
  https://www.icann.org/en/system/files/correspondence/marby-to-cooper-kuhlewind-22oct20-en.pdf

  Answer from the IETF on 13 Nov 2020.
  https://datatracker.ietf.org/liaison/1706/

- We are to do data analysis on data sensitivity and ensuring dns queries from specific points in dns hierarchy impact ability to determine name collision impacts.

- Jim: we should call attention to 3 cases:
    - Legacy: corp/home/mail
    - Special Use domains: IETF relationship with ICANN: .onion
    - Squatters: .crypto….ICANN needs to determine how to deal with them. Can .crypto allow .crypto to buy it but prevent anyone else from buying it?

ACTION ITEMS

#	Action Item
1	Amy to research if there was any further follow-up to the letter exchange between Goran Marby and IETF regarding SAC113.