Team Meeting - Workshop

17 NOVEMBER 2020

Attendees

Tim April

Gavin Brown

John Crain

Merike Käo (coordinator)

Rod Rasmussen

Marc Rogers

Katrina Sataki

Robert Schischka

Duane Wessels

Heather Flanagan (ICANN support, technical writer)

Steven Kim (ICANN support, project management)

Wendy Profit (ICANN support, project management support)

Samaneh Tajalizadehkhoob (ICANN support, technical support)

Regrets

Sally Newell Cohen (ICANN support, communications)

Agenda

Introduction:

1. Objectives of the workshop
2. Expected outcomes
    - Spreadsheet that list all the consolidated successful attack vectors
    - Time permitting, spreadsheets that will enumerate mitigations and gaps

Session 1:

3. Compare the campaigns discussed so far and enumerate causes that allowed the attacks to be instantiated.

    - Have we captured enough?

4. Work through the attack vectors used for each campaign.
5. Can we distinguish more prevalent attacks?
6. Document commonalities in attack vectors
7. Discuss mitigations

BREAK

Session 2:

8. Continue discussion on mitigation of attacks
9. Identify main gaps

Notes

- **The TSG reviewed different attacks on the DNS with the goal of building a taxonomy of attack vectors. This will be used to build a future list of potential mitigations.**
    - The TSG worked with the campaigns previously identified by TSG members to develop the high-level categories of attack vectors.
    - The TSG discussed additional attack campaigns and vectors in areas that were listed in the Charter but not yet considered in the list of exemplar attacks.
- Next steps
    - The TSG will finalize the list of attacks and attack vectors, and consider what mitigations are possible.

Action Items

1. ICANN staff to find a diagram of the ecosystem, (DNS Components diagram)
2. ICANN staff to save reference documents to the shared folder.
3. ICANN staff support will build a high-level list of attack vectors for the TSG to review. The TSG will be asked to prioritize this list from the perspective of the biggest problem(s) for security in and around the DNS ecosystem, and to bring their thoughts to the next meeting.