cloud security alliance®

Cyber Threat Psychology Research Working Group

Proposal / V1.1, Release Date: 31/10/2024

Cyber Threat Psychology Working Group

Overview and Audience

Overview

A cyber attack involves multiple actors whose motivation, thinking, behaviours and experiences often are going back into early childhood of all actors. For a cyber attack to succeed, the transmission mechanisms and the communication aspects are of equally relevant importance.

This research stream of the CSA Swiss Chapter is looking into both the originating "supply" side and the "receiver" side of hacktivism, plus the transmission, communication and influencing mechanisms.
Objectives and focus areas are:

- The psychological motivations of attackers
- Their origins from personal conditions, social context and behaviour
- The transmission mechanisms: subversion, deception, poisoning
- Ways for interception at "Supply Side"
- Potential approaches how to influence behaviours of attackers to turn them into positive constructive contribution rather than negative harmful destruction
- Potential behavioural change at "Receiver Side" to understand the background of hacktivism, to develop and to apply communication, social, emotional awareness and better detection and response.
- Changing the incentive patterns and mindsets of both the "supply side " and the "receiver side" to reduce attacks and impact.

Audience

Proposed Working Group Members

CSA Global Management

CSA Research Management

CSA Swiss Chapter Board

Cyber Threat Psychology Research Stream: Abstract

A cyber attack involves multiple actors whose motivation, thinking, behaviours and experiences often are going back into early childhood of all actors.

This research stream of the CSA Swiss Chapter is looking into:

The “supply side”:

- The psychological motivations of attackers.
- The origin of these motivations.
- Potential approaches how to influence behaviours of attackers to turn them into positive constructive contribution rather than negative harmful destruction.

The “transmission and “communication” aspects:

- Undermining with subversion
- Influencing with deception
- Acting with poisoning: “Psychology as a Weapon” and “Code as a Weapon”

Cyber Threat Psychology Research Stream: Abstract

The “receiver side”:

- How to approach mindsets of those who may be attacked in order to pre-empt and prevent attacks from being successful.
- Voice from the Top: How lived social, leadership and management behaviour can change the motivation of everybody in a state, community, firm.
- The behaviours of those when under attack, as these may significantly change how severe the impact of the attack will be.

Cyber Threat Psychology Research: Objectives (1/3)

Research into Cyber Threat Psychology is aiming at:

1. Identifying personal conditions which foster the development of behaviours ultimately being deployed to hacktivism: shyness, genius, one-sided excellence, isolation, social media consumption, strength, …
2. Identifying social context conditions which foster the development of behaviours ultimately being deployed to hacktivism: neglect, lack of appreciation, bullying, mobbing, skills not being recognized, the power of words, social environment, political system, chance equality, …
3. Analysing the transmission mechanisms at the “supply side”: most people in the same constellation don’t develop the negative mindset of hackers. What are combinations of factors resulting in evil mentality?
4. Identifying potential interception points and mechanisms “supply side”:
    a) Which of the above conditions and transmission mechanisms are suitable to interfere with?
    b) What possible interference patterns and approaches exist and how can these be tuned to achieve positive outcome?
    c) Longer term approaches to impact change in the conditions to prevent them from fertilising hacktivism mindset
    d) “Social engineering”: target potential or actual Hackers and their social environment via the conditions and transmission mechanisms identified in this research project, to approach them and effect a mindset change

Cyber Threat Psychology Research: Objectives (2/3)

Research into Cyber Threat Psychology is aiming at (continued):

5. Analysing and identifying interception points in the transmission mechanisms between the “supply side” and the “receiver side”:
    a) Undermining with subversion: Underground agitation to seed fear and destabilise, influencing elections, trolls seeding “alternative facts” and misinformation, intrusion into social channels, etc.
    b) Influencing with deception: working actively on the population by e.g. disseminating false information which is attributed to official channels or persons, intruding into public networks, etc.
    c) Acting with poisoning: “Psychology as a Weapon” and “Code as a Weapon”: targeting the broad public or specific important / highly respected individuals with psychological means to poison their opinion and to leverage them thereafter as opinion leaders to achieve wide spread poisoning. Weaponising code of trusted news feeds, fora, social media to further inject and spread poisoned information to poison the receiving society.

Cyber Threat Psychology Research: Objectives (3/3)

Research into Cyber Threat Psychology is aiming at (continued):

5. Identify action points on the “receiver side”:
    a) Society and Communities: How does a state’s society respond to the communication received via the transmission channels, in particular to the subversion, deception and poisoning triade? Can this be improved, sharpened, immunised by appropriate awareness and information / education campaigns? How can state / community leadership impact and positively influence this?
    b) Corporates: Top Management culture and behaviours exemplarily demonstrated
    c) Corporates: Organisational change: modifying processes, incentives and organisational mindset to effect a culture change
    d) Corporates: All staff awareness: understand the background of hacktivism as per this research project, develop novel training and real live awareness programs, apply social and emotional awareness
    e) Private Individuals: awareness activities to help identifying potential persons in the personal environment who could become susceptible to developing into hacktivism, and to coach or encourage them to change mindset or route
    f) Institutions: educate to overcome the often lack of understanding of exposure to cyber attacks, social engineering, indirect exposure via careless information sharing or unconscious biases of trust, and their transmission mechanisms
    g) All: Behaviour change: how to apply curiosity and social / emotional awareness and turn it into mischievous vigilance to prevent being caught by hacking

Cyber Threat Psychology Research: Structure Proposal (1/2)

Proposed Research Streams:

A. Personal Conditions and Behaviour

B. Social Context and Behaviour

C. Transmission Mechanisms

D. Communication, information, education

E. Interception at "Supply Side": possibly split into Hackers, Environment

F. Behavioural Change at "Receiver Side": possibly split into All, Corporates, Institutions, Privates

Cyber Threat Psychology Research: Structure Proposal (2/2)

Proposed Activities:

- Integration with research projects and activities in Psychological and Cyber Defence Agencies, Universities, private Research / Think Tanks
- Interviews with ethical hackers: learn from their motivation and their approaches
- Engage with HackerOne and other ethical hacking companies : deep dive into background of attacks, motivation, approaches to identify early and work on incentivising hackers to change mind / side
- Interviews with youth psychologists: behavioural and motivational aspects
- Interviews with senior psychologists analysing the information and behaviour patterns of the broader public and society
- Interviews with sociologists: impact from social context, environment and behaviour
- Interviews with behavioural scientists: understand the transmission mechanisms, ways towards mindset changes
- Engage with SOC Working Group of SIGS: Receiving Side Patterns
- Engage with Pen Testing Companies: Corporate Behaviour in response to pen test results
- Engage with CISOs and CEOs: Corporate Behaviour, Corporate Culture, actively living and demonstrating exemplary behaviour of vigilance based on understanding the emotional and mindset background of hacktivism
- Engage with Cyber Criminologists: learn from real cases and personal situation / behaviour and context observed

What's next

Proposed Next Steps:

- Reach out to all proposed Working Group members and confirm their participation
- Define Charter of proposed Working Group, have all members to endorse
- Formally establish Working Group at CSA Global
- Set up fortnightly Working Group calls
- Working Group Initiation Meeting to establish streams and constituency, deliverables, timelines and ownership