# **Adversary engagement** v prostředí **SeGC**

MIKULOV ☐ **05.09.2023**

SPCSS

Státní pokladna
Centrum sdílených služeb

# Disclaimer

This presentation is in English.

This presentation was not created by the vendor or AI ☺

Mentioned research is hypothetical.

# Adversary engagement v prostředí SeGC

# Our research

# Our research

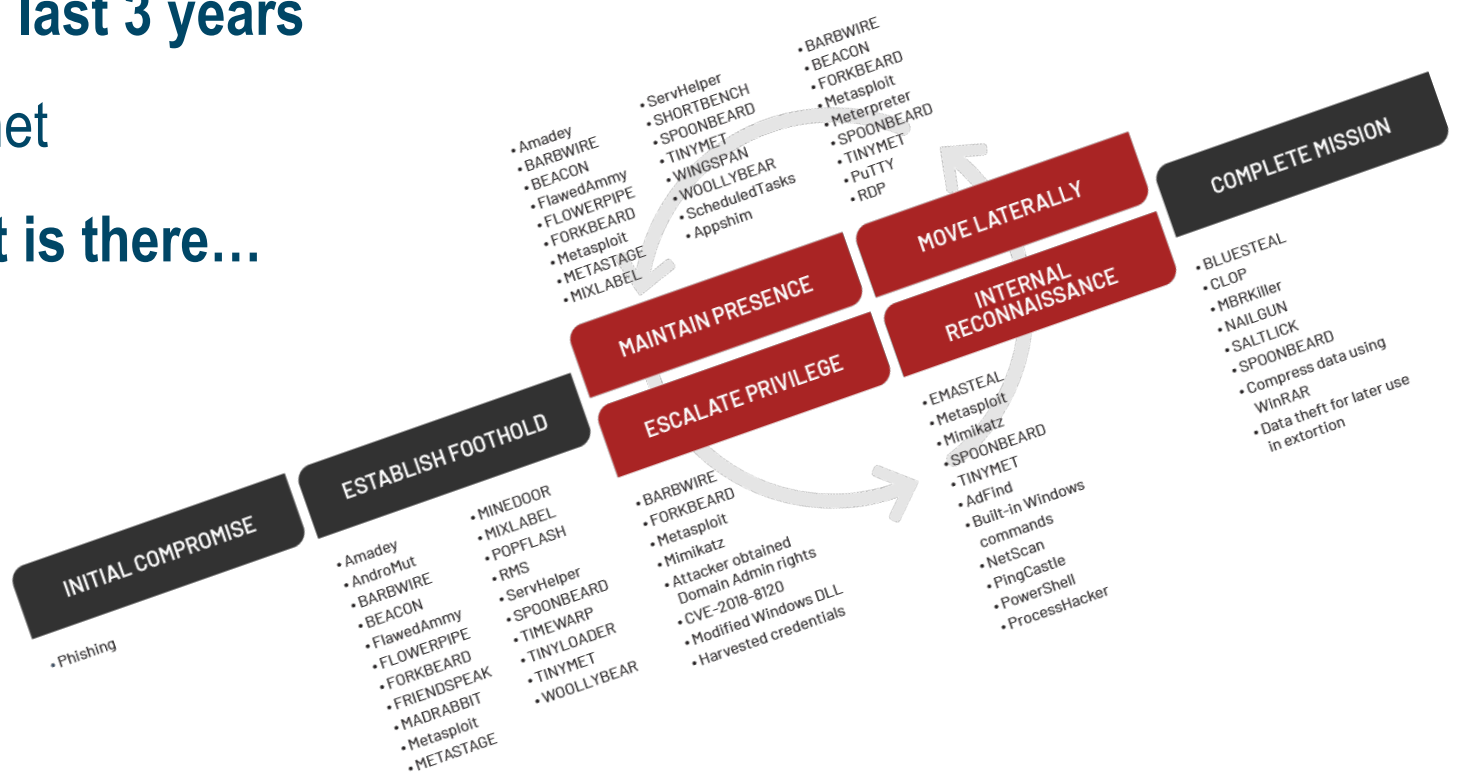
## Research inspiration

- Based on our CTI research.
- What government‘s domains are contained in leaks?
- No users!

# Our research

## Where?

- **Available in our research pool:**
  - 120 billion records in **last 3 years**
  - I2P, DarkWeb, Internet
  - **No one cares, but it is there…**



# Our research

## Hypothesis

- Can we get number of Gov leaked domains?
- What is number of leaked government‘s domains and positive founds?

# Our research

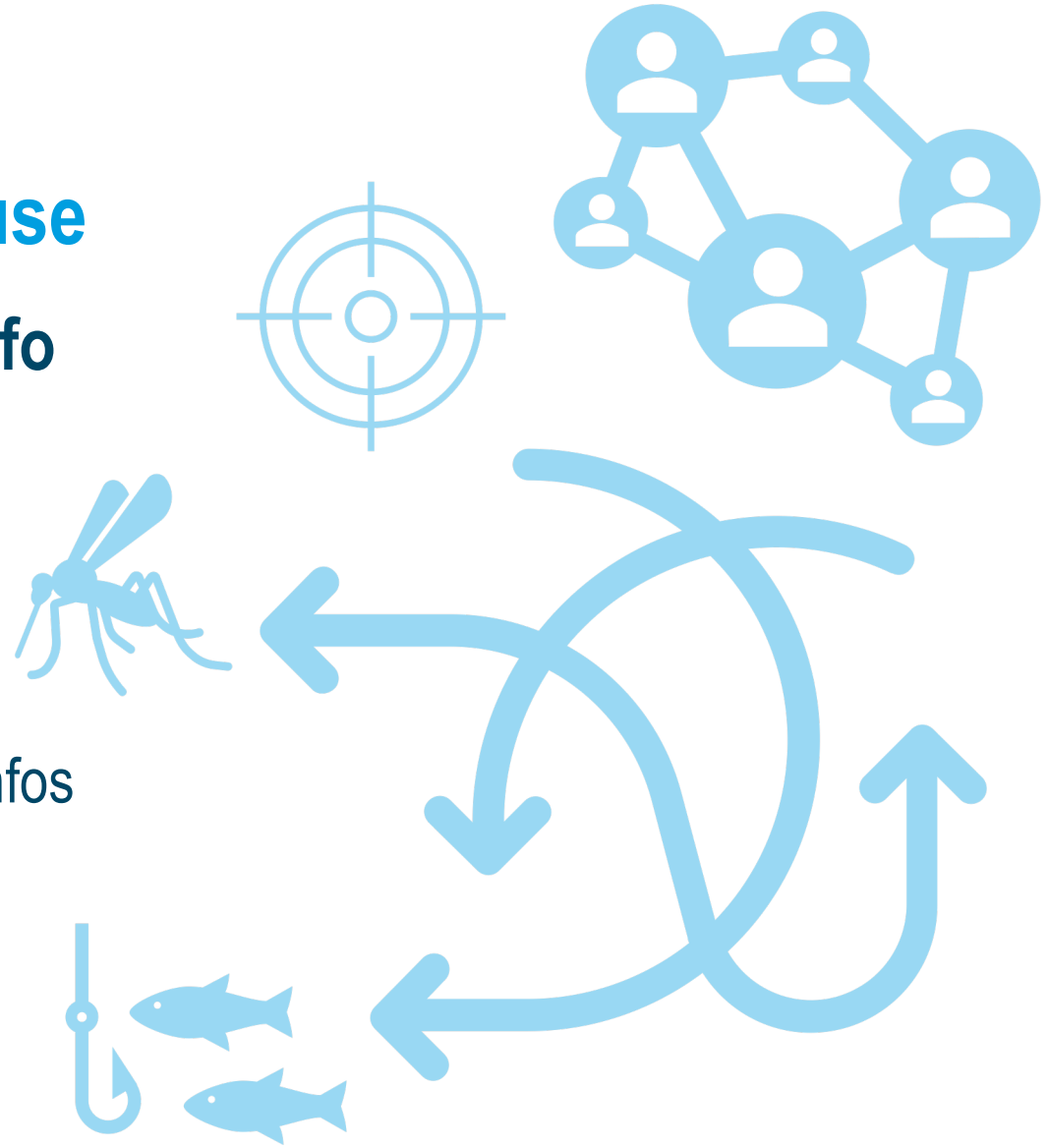
## Research goals

- Our domains leak monitoring
- Preventing abuse

# Our research

## Attack procedure for User abuse

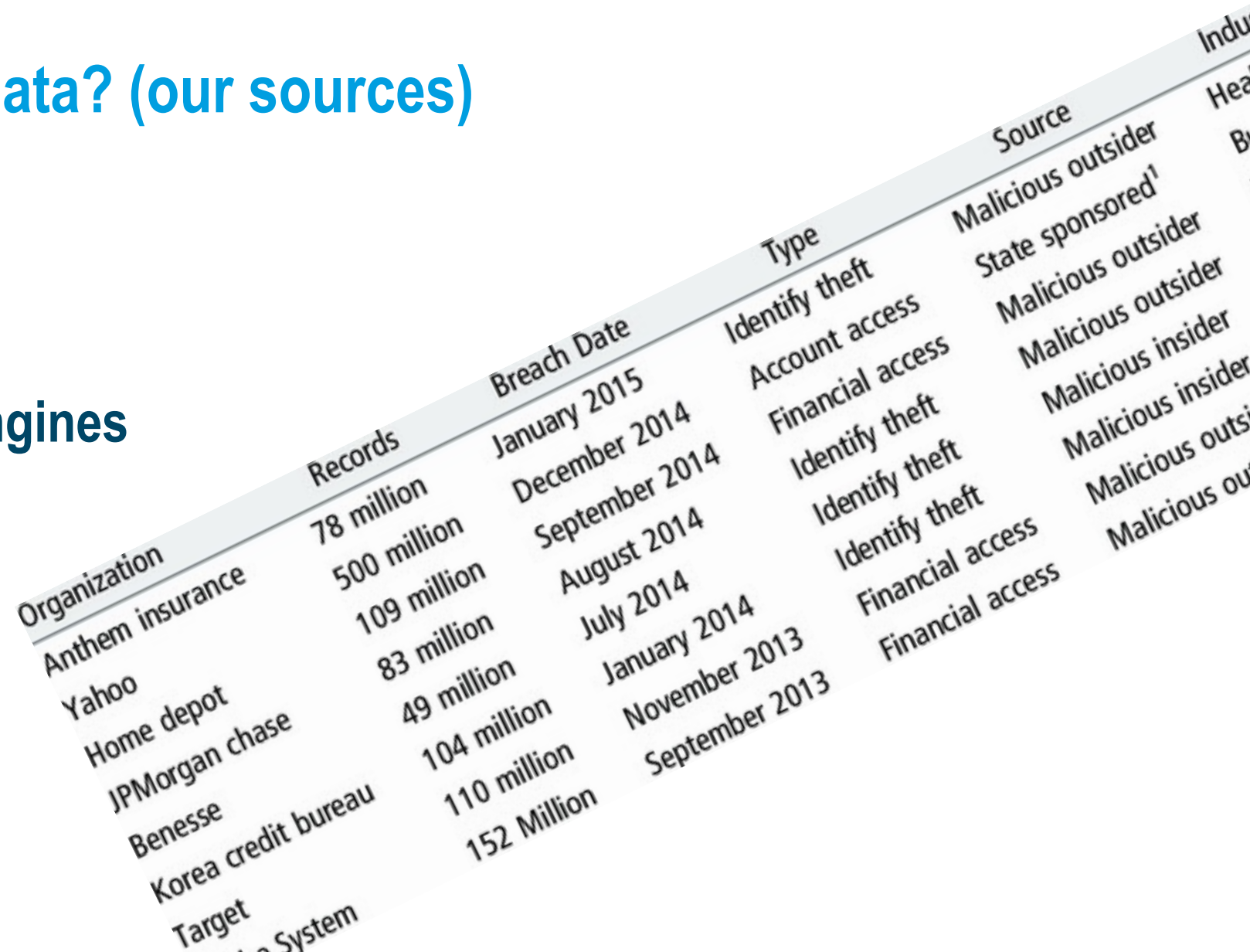
- **Get user (username and pass) info**
  - …not only (browsers, pc names, nicknames, address…)
- **Social digging**
  - To deep context in social networks infos
- **Phish user**
  - Interaction with target
  - Getting access



# Our research

## Where to get data? (our sources)

- Leak forums
- DarkWeb
- Leak search engines



| Organization | Records | Breach Date | Type | Source | Indu |
|---|---|---|---|---|---|
| Anthem insurance | 78 million | January 2015 | Identify theft | Malicious outsider | Hea |
| Yahoo | 500 million | December 2014 | Account access | State sponsored[1] | B |
| Home depot | 109 million | September 2014 | Financial access | Malicious outsider | |
| JPMorgan chase | 83 million | August 2014 | Identify theft | Malicious outsider | |
| Benesse | 49 million | July 2014 | Identify theft | Malicious insider | |
| Korea credit bureau | 104 million | January 2014 | Identify theft | Malicious insider | |
| Target | 110 million | November 2013 | Financial access | Malicious outsi | |
| System | 152 Million | September 2013 | Financial access | Malicious ou | |

# Our research

## Armory (Tools)

- **Hlídač Státu API**
  - All Government domains list
  - First helpful use of EVER

  (for both sides of the Force)
- **Search engines API**
  - Gathering data programatically

# Our research

## Armory (Tools)

- **ChatGPT for scripting**
  - For better sorting domains
- **From days to minutes**
  - Manually vs automate for social digging

# Our research

## Our OWN solution

- Dr4cula665
- DarkWeb, Pastebin monitor
- Web scrapper
- Alerting
- Homemade
  - For SPCSS only
- Feel free to ask Us

# Our research

## Results - numbers

- Leaks in last 3 years
- 50 000 + Czech Gov domains records
- 22 274 unique Czech Gov domains records

# Our research

## Results – numbers

- SCOPE - leaks contained users and pass

- SPCSS – 0 records

| | |
|---|---|
| cuzk.cz | 1995 |
| mvcr.cz | 1995 |
| cssz.cz | 1882 |
| plzen.eu | 1856 |
| msmt.cz | 1576 |
| mfcr.cz | 1433 |
| mze.cz | 1387 |
| kr-ustecky.cz | 1285 |
| kr-jihomoravsky.cz | 1277 |
| ctu.cz | 1246 |
| vlada.cz | 1137 |
| dpp.cz | 1134 |

# Our research

## Whats the problem?

- Main - Database breach
  - Database owner problem
- Users problems…
  - Password re-use
  - Password complexity very low
- **Why it get to databases?**
  - Work email use for Netflix and others…

# Adversary engagement
v prostředí **SeGC**

# Thats not all

# Adversary engagement
v prostředí **SeGC**

## About Us

- **Ondřej Nekovář**
- CISO, CDO
- Wide aimed

@th30ne__

- **Jan Pohl**
- Threat hunter, Practical CISO advisor
- Deep aimed

@adversary_mr

# Adversary engagement
v prostředí **SeGC**

## About Us

- **Ondřej Nekovář & Jan Pohl as speakers**
- 6 years
- Own research – **ACD**, **Deception**, **Detection engineering**
- BlackHat, QUBIT and many others
- DeceptionDigest.com

# Our environment

SPCSS
Státní pokladna
Centrum sdílených služeb

- **State company**
- **Critical information infrastructure**
  - And all measures (ISO 27x…SOC2)
- **SeGC**
- **Cyber Security Services**
- **Hybrid environment**
  - on-prem, Azure, AzS, GC, AWS

# Our strategy

- Internal resources
- Own R&D
- No vendor dependency
- Pro/active attitude
- CTI, Deception, Detection, AI ☺
- Cooperation

# Our team

## Cyber Security Division

- Internal staff: **27**
- L1 SOC (24x7): **12**
- Trainees: **2**

- Open FTE: **4 (2023), 11 (2024)**

- **SOC (7 plus 12), CTI unit (4)**

# Our projects

- **Project B** (people)
- **Project E** (endpoint)
- **Project M** (communication)
- **Project S** (deception)
- **Project Z** (management)

# Adversary engagement
v prostředí **SeGC**

# Active Cyber Defense

# Active Cyber Defense

## Why to use ACD?

- **Early detection**
- **Very low false positive detection ratio**
  - vs Reactive detecion.
- **Excelent detection engineering supplement**
  - e.g. covering blind spots.
- **Doesn't require deep understanding**
  - of technologies.

# Active Cyber Defense

## How to present ACD in technical way?

- **Individual**
  - **Decoys** (Assets)
  - **Lures** (Services)
  - **Breadcrumbs** (all activities traces)

**vs**

- **Whole deceive systems and networks**

# Adversary engagement v prostředí **SeGC**

# Active Cyber Defense Gray Zone

# Active Cyber Defense

## ACD‘s place in the order

| | |
|---|---|
| **Reactive defense** | Antivirus, Firewall, SIEM, incident response ... |
| **Active defense (Gray zone)** | **Pro-active, Elements, Beacons, Deception, Emulation, Hunt…** |
| **Offensive operations** | Hacking back, cyber operations ... |

# Active Cyber Defense Gray Zone

## How to use categorize ACD?

| | |
|---|---|
| Adversary emulation | Adversary Takedowns |
| Beacons | Ransomware |
| Deterrence | Rescue Missions |
| Deception | Sanctions, Indictments & Remedies |
| Tarpits, Sandboxes & Honeypots | |
| Threat Intelligence | |
| Threat Hunting | |

Assembled by DCG420

# Active Cyber Defense Gray Zone

## ACD Gray Zone Shortcomings

- ACD Gray Zone was not comprehensive for practical use.
- We need to rework each category into a process…

# Active Cyber Defense Gray Zone

## What activities we wanted to include in the process

- **Detection engineering**
- Use of **CTI**
- Threat **modeling**
- Threat **emulation**
- Threat **hunting**
- Observing **threat landscape**
- Possible **external attack vectors**
- **Active countermeasures** use **(deception)**

# Active Cyber Defense Gray Zone

## Process Goals

- **Application of ACD Gray Zone elements**
- **Killchain mapping**
- **Combination of ACTIVE plus PRO-ACTIVE plus REACTIVE elements**
- **Documentation** (inputs, outputs)
- **Decision making** support
- Custom **risk assessment**
- **Improvement = Loop = Repetition = B.A.U.**

# Adversary engagement
v prostředí **SeGC**

## ACD Loop = process

# ACD LOOP Definition

## ACD Loop

1. **CTI Input** (threats)
2. **Analyze** (risks analysis)
3. **Model** (testing scheme)
4. **Verify** (detection test execution)
5. **Tune** (detection engineering, blind ACD)
6. **Validate** (test 2)

# Adversary engagement
v prostředí **SeGC**

## Research in ACD Loop

# Research in ACD Loop

## How we get results in useful way?

## ACD Loop

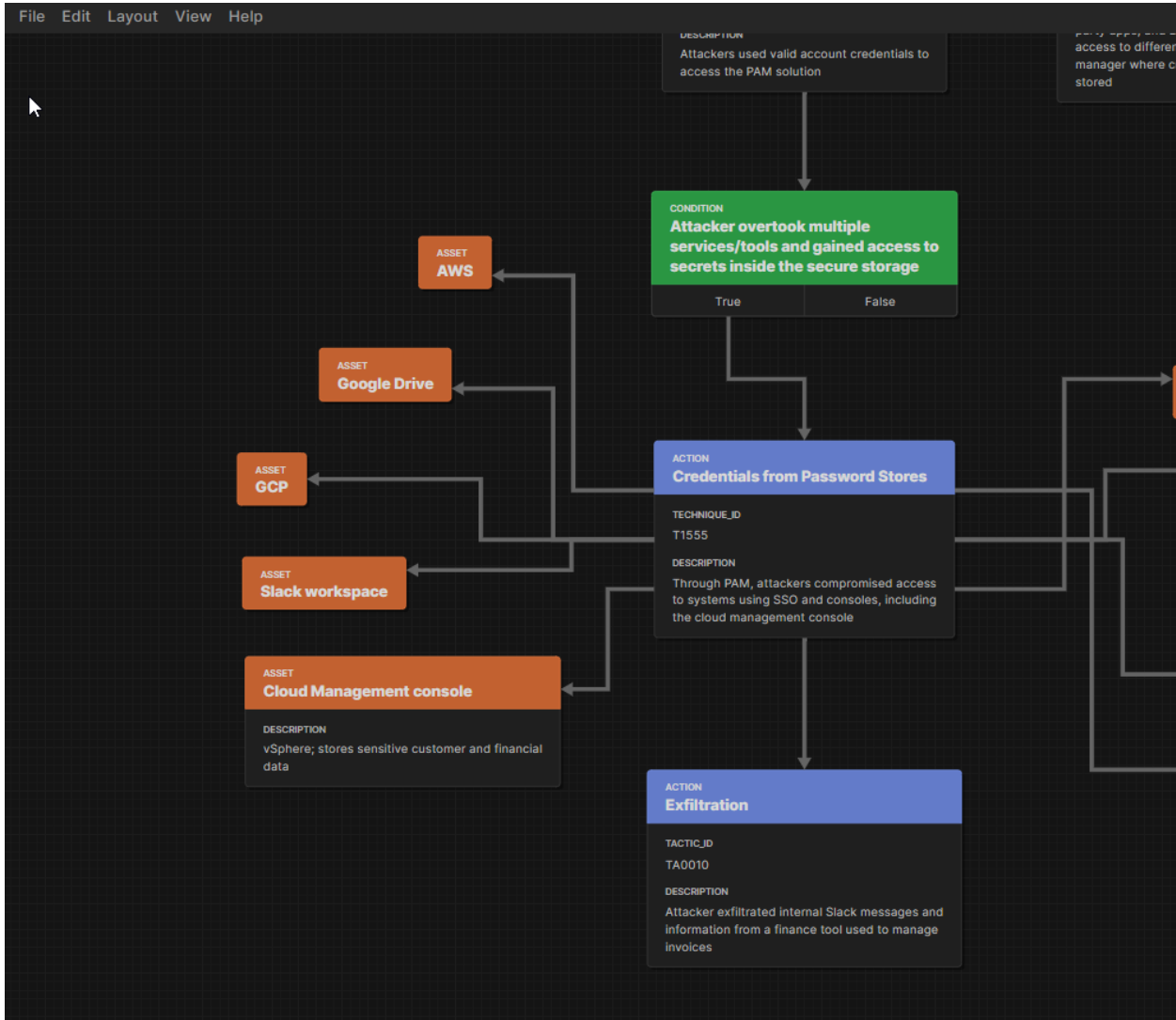
1. **CTI Input**
   - Retrieve as many **information** as possible about **domains leaks/abuse**
2. **Analyze**
   - Domains leaks **risk evaluation**

# Research in ACD Loop

## ACD Loop

### 3. Model

- **Graphical expresions** of threat



# Research in ACD Loop

## ACD Loop

### 5. Verify

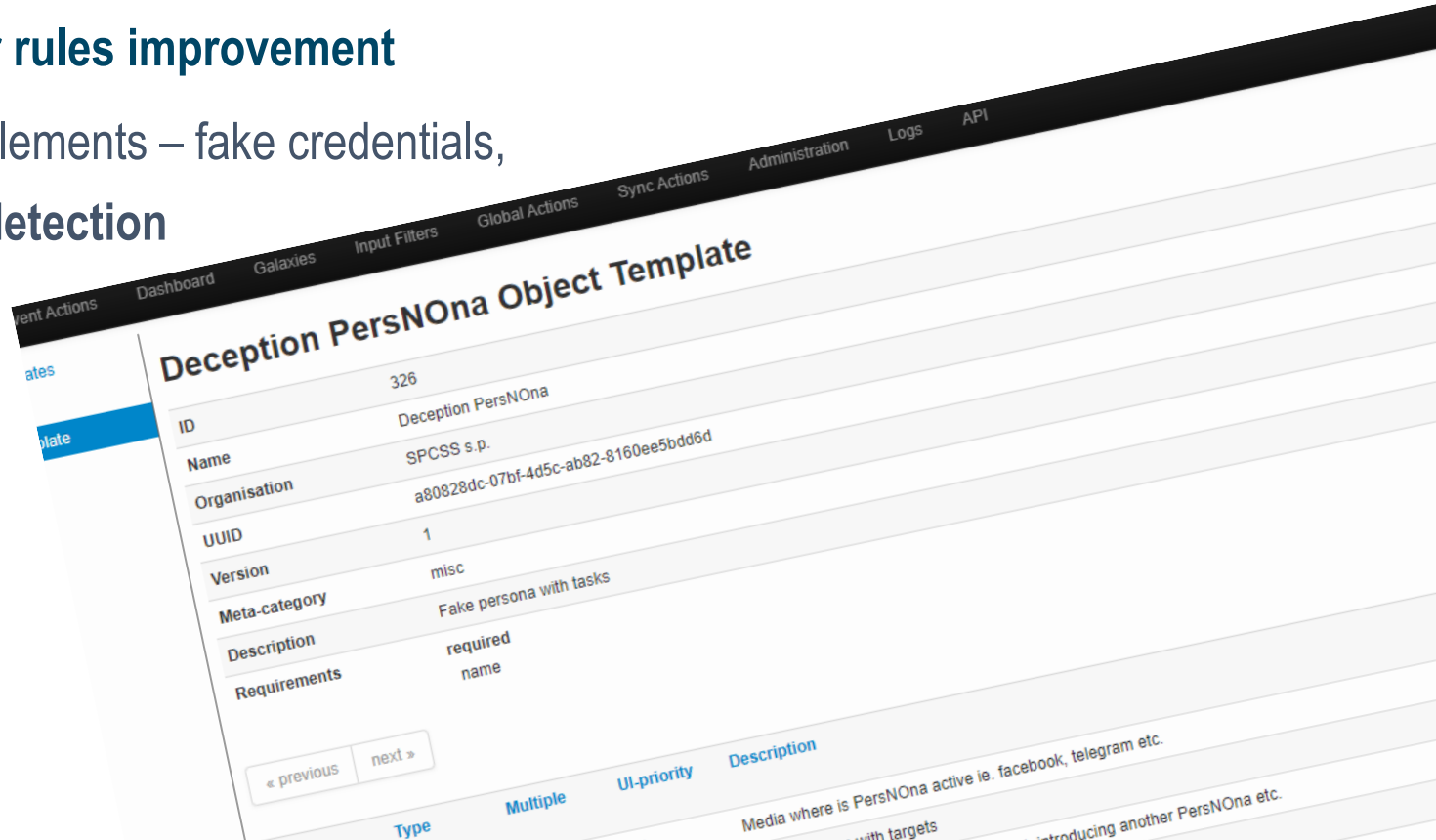
- **Evaluation** of current status
- Leaks found
- Detection for user data abuse

# ACD LOOP Definition

## ACD Loop

### 5. Tune

- Detection engineering for **rules improvement**
- Implementation of ACD elements – fake credentials, fake personas for **early detection**



# ACD LOOP Definition

## ACD Loop

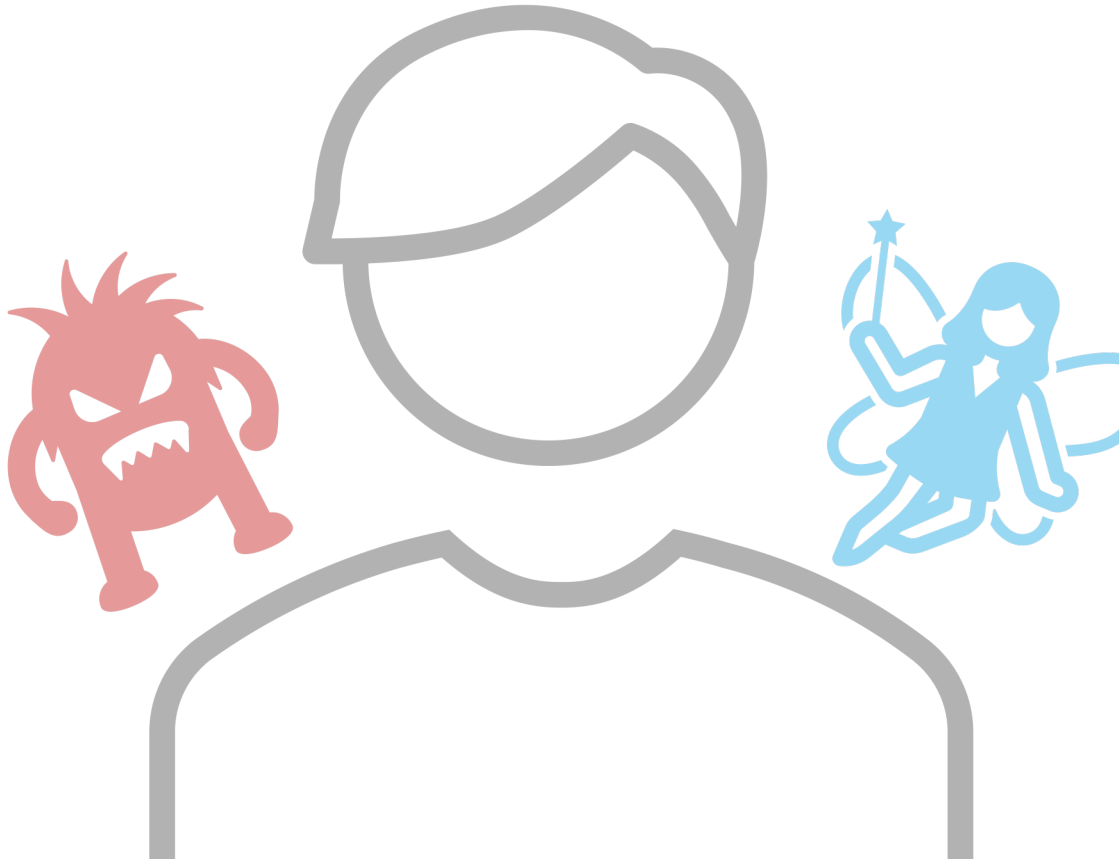
### 6. Validate

- **Adversary emulation** for domains abuse
- Leaks, fake credentials, fake personas **monitoring**

# Take aways

# Take aways

- **Monitor** your **domains**.
- **Easy** to manage and „**free**“.
- Mind the **legal issues** with users data.
- **Train** your **staff**. (no Netflix)
- **Train** you **management**.
- **Do not trust anyONE!**




Adversary engagement
v prostředí SeGC
EoF

# Our activities

- **Active Cyber Defense and Deception Workshop**
  - November 2023, Prague
  - In English

# Our activities

- **Engage: Miluj svého protivníka (Workshop)**
  - **12/9/2023** 12:00-16:00, NÚKIB CyberCon Brno
  - Techniques for deploying ACD elements

- **Analýza rizik veřejných zakázek (Přednáška)**
  - **13/9/2023** 10:10-10:30, NÚKIB CyberCon Brno
  - Představení průvodce NÚKIB a SPCSS

- **CTI Summit/Hack.lu LUX**
  - **RUS/UKR conflict impact on cybersecurity**
  - October 2023

- **Fórum aktivní kybernetické obrany 2024**

spcss.cz/**cloud**

# Sledujte nás

**18.10**

Gajdošův sál

**eGC KALKULÁTOR**

**15.50**

Gajdošův sál

**MODERNÍ TECHNOLOGIE F5 V CLOUDOVÝCH PROSTŘEDÍCH**

# Stay in touch

www.spcss.cz/FAKO

www.spcss.cz/CSIRT

csirt@spcss.cz

@csirtspcss

# Thank you!