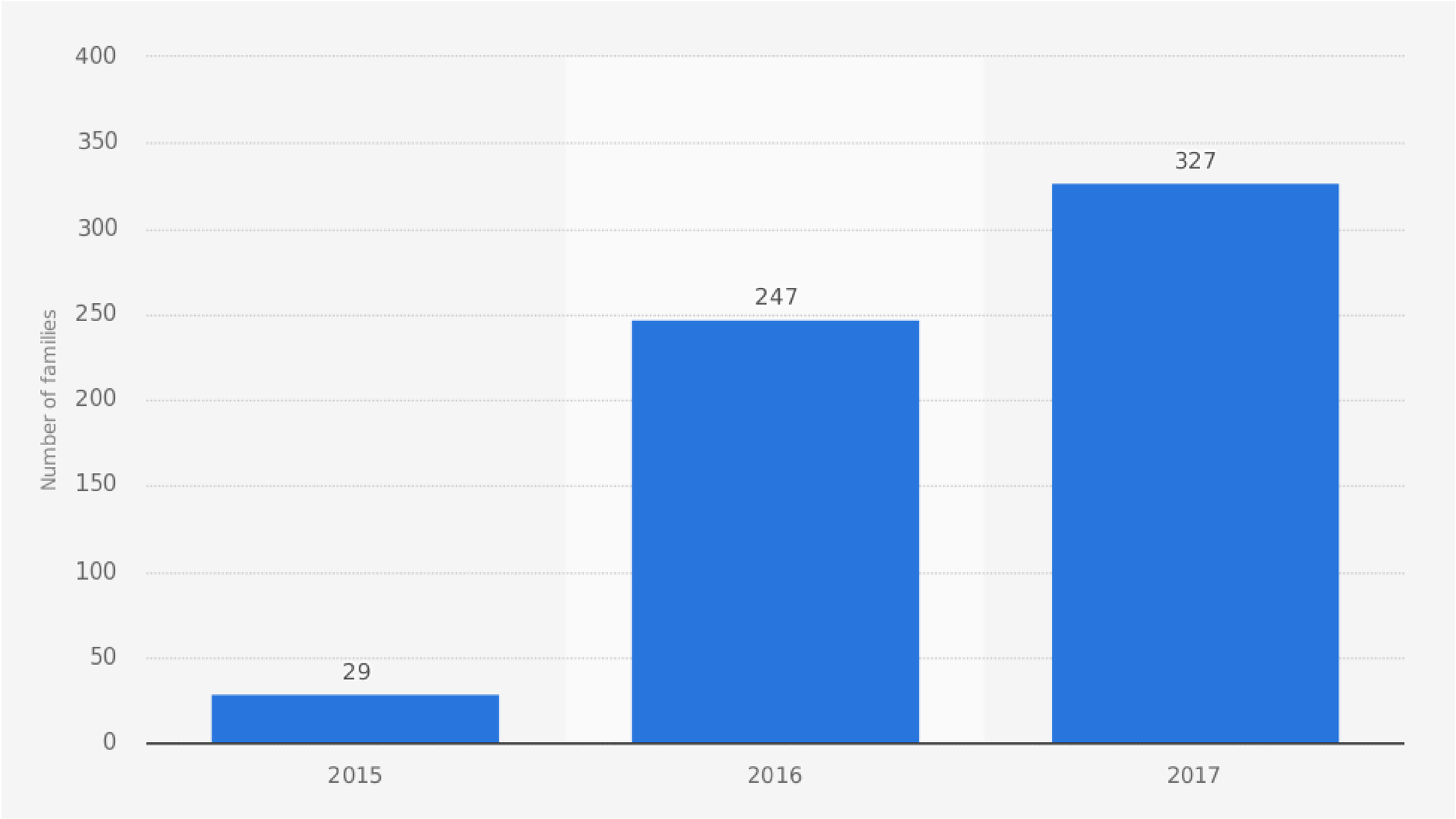
Behaviorálne aspekty vybraných častí ransomware

Júlia Kázsmérová

Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.
Konzultant: Mgr. Ladislav Bačo

Motivácia


400
350
300
250
200
150
100
50
0
Number of families
29
247
327
2015
2016
2017

Ciele práce

Analyzovať ransomvér a jeho známe typy

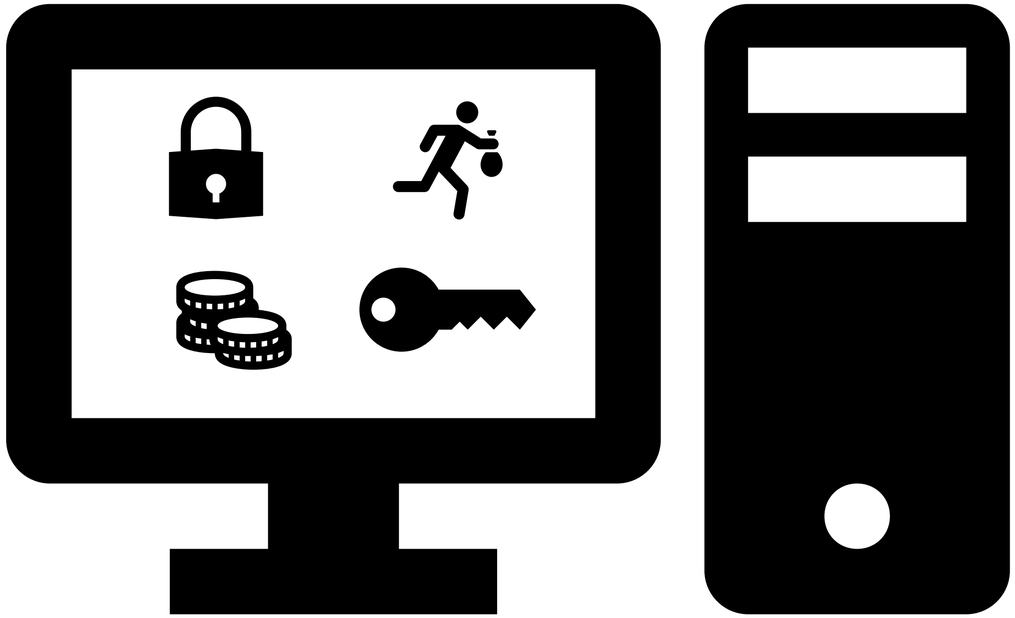
Porovnať jednotlivé prístupy k analýze ransomvérov

Navrhnúť a porovnať metódy detekcie a obrany voči ransomvér

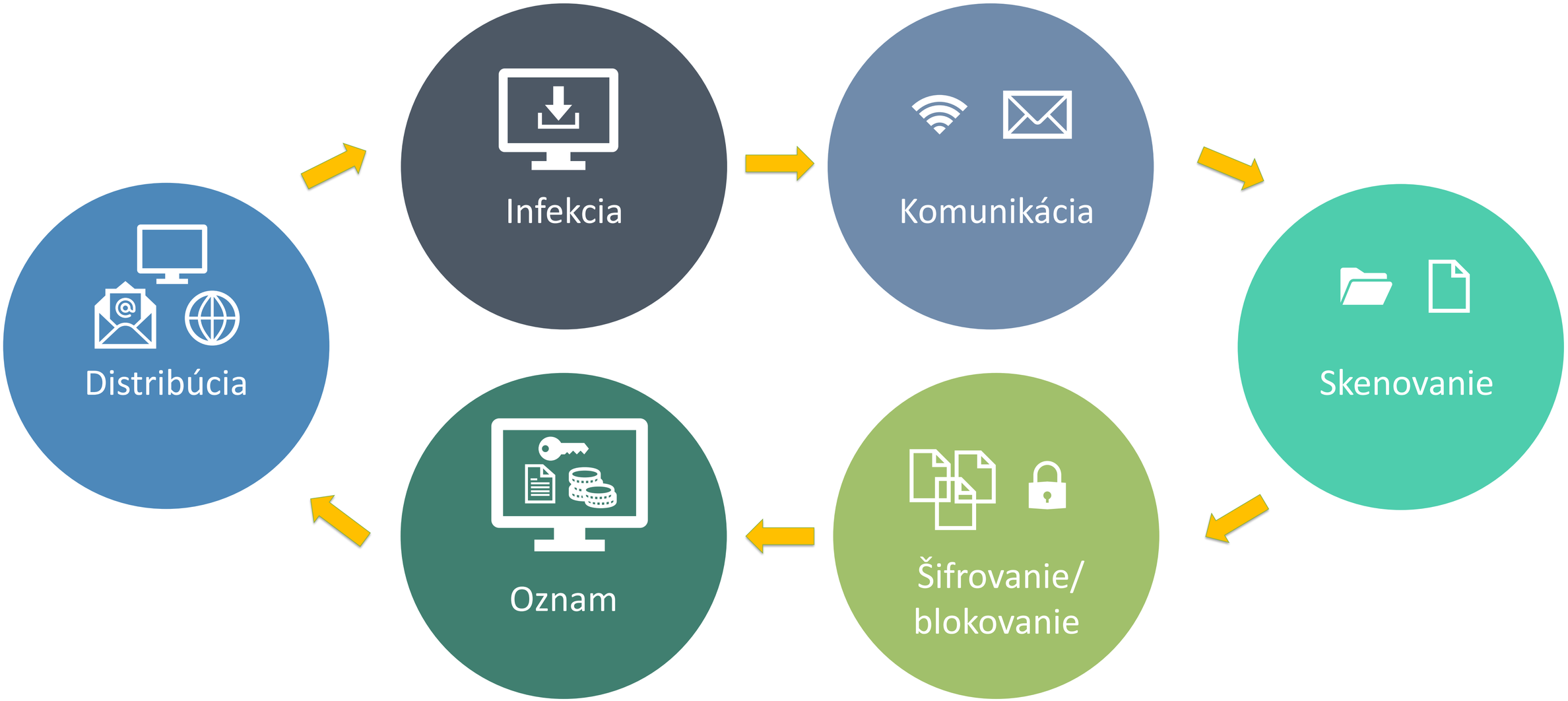
Návod na konfiguráciu domáceho laboratória na analýzu ransomvér pomocou Cuckoo systému

Ransomvér

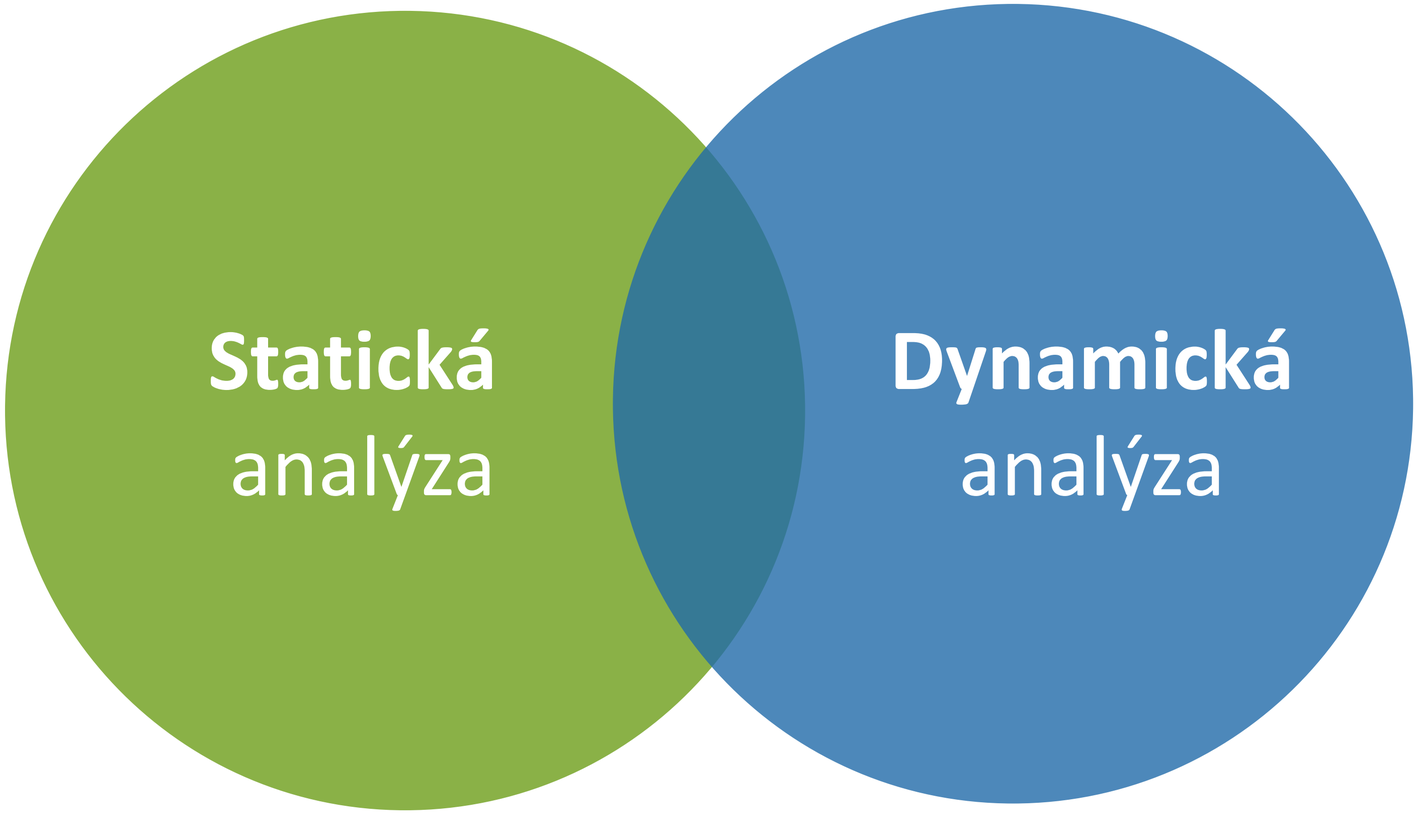
- Ransom + ware
- 1989
- Šifrovací a blokovací



Vykonávané kroky



Typy analýz ransomvérov



Analýza ransomvérov je proces, pomocou ktorého sú skúmané vzorky ransomvérov, aby sme lepšie pochopili ako fungujú, aké škody môžu spôsobiť, ako sa dajú odhaliť a ako sa môžeme voči ním brániť.

Nástroje pre analýzu malvérov

	Statická analýza	Dynamická analýza	Strojové učenie
Maltester	X	X	
HELDROID	X	X	
EldeRan		X	X
UNVEIL		X	

- Voľne dostupný automatizovaný bezpečnostný systém
- Google Summer of Code, 2010
- Súbory, dokumenty, webové stránky
- Behaviorálne vlastnosti, sieťová komunikácia, screenshoty, ...

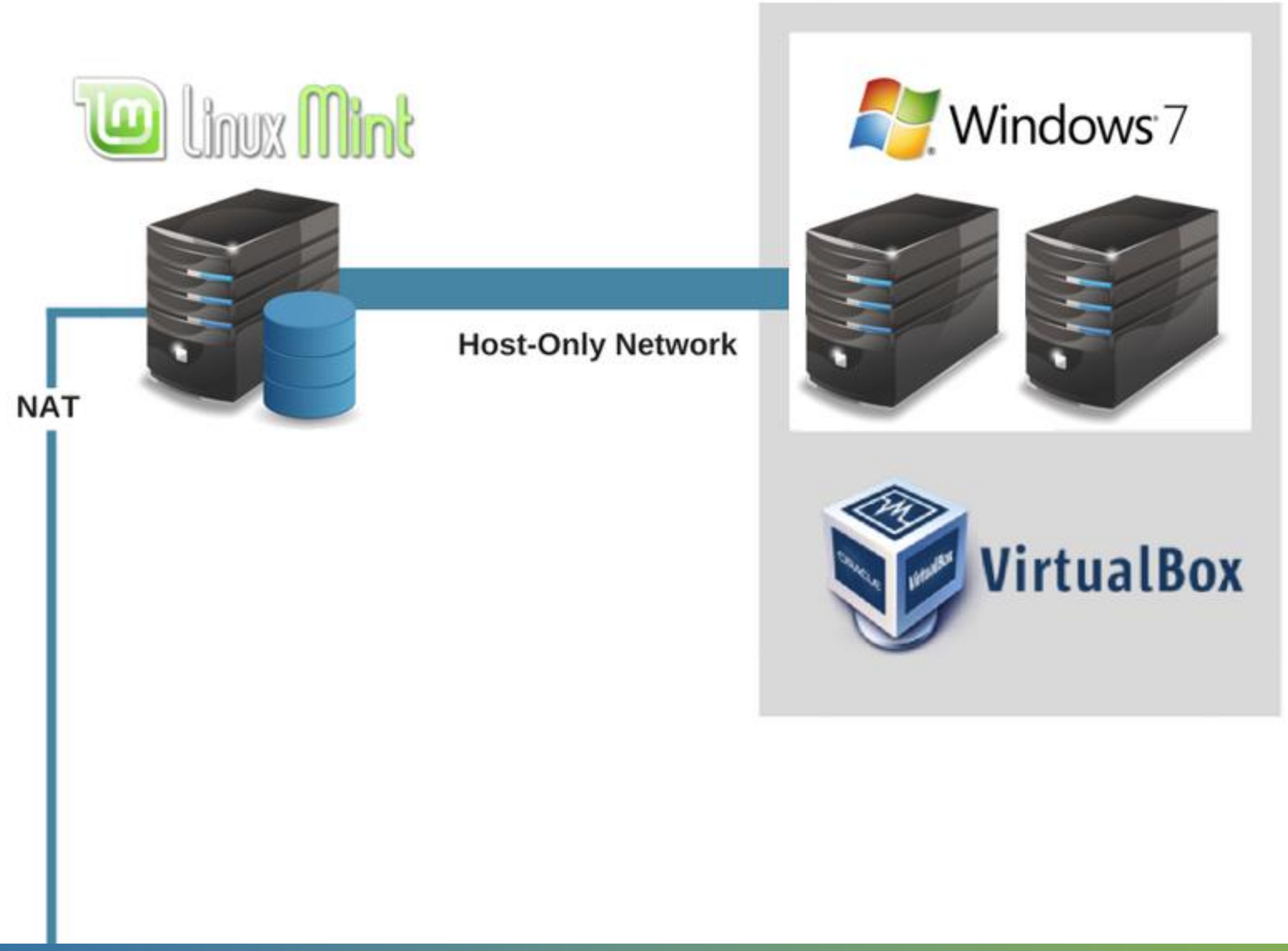
Dataset

- 12. – 14.03.2018
- 153 000

  → .exe: 64 000
  → .json: 89 000

- „ransomware“
- 5 227

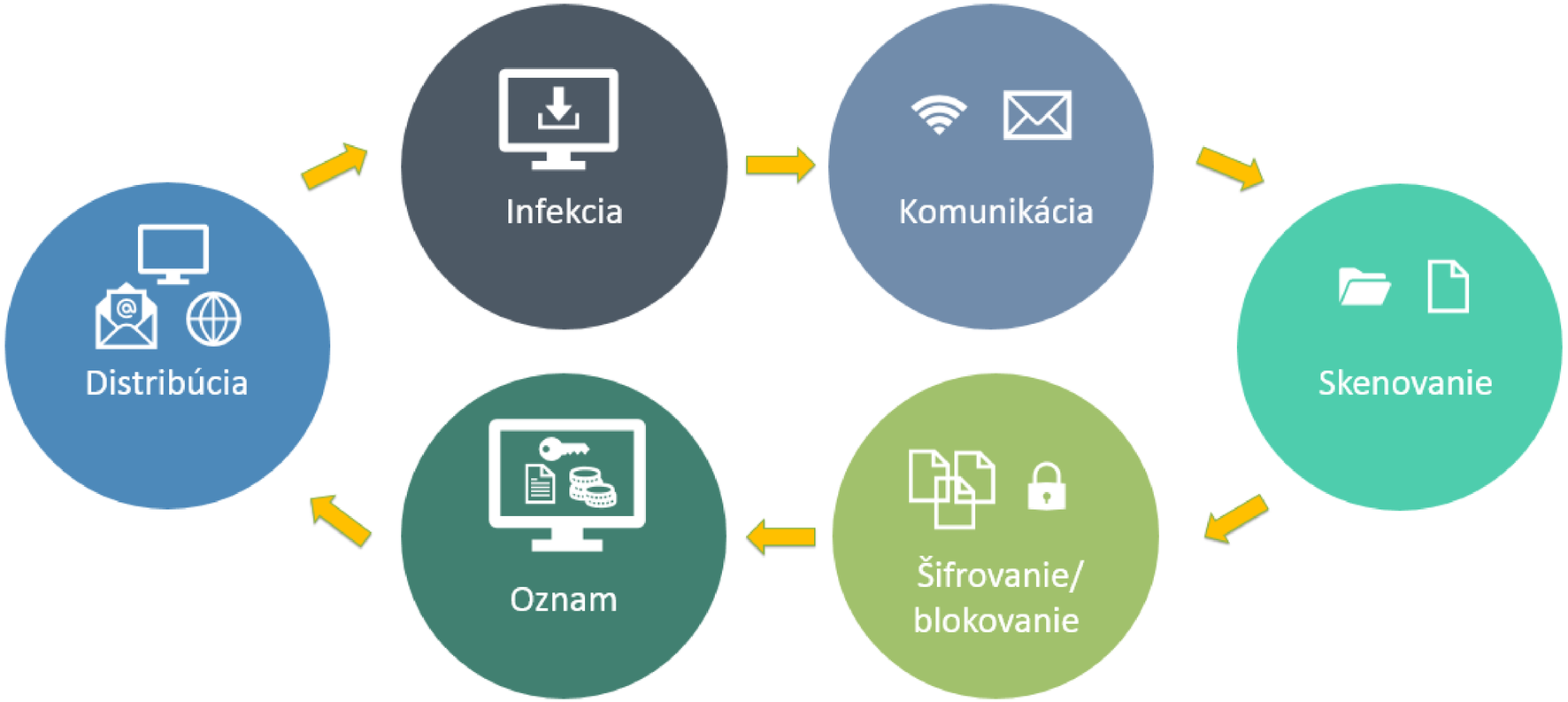
Architektúra prostredia



- Typy súborov
- Umiestnenia
- Zdieľané priečinky
- Sieťové nastavenia

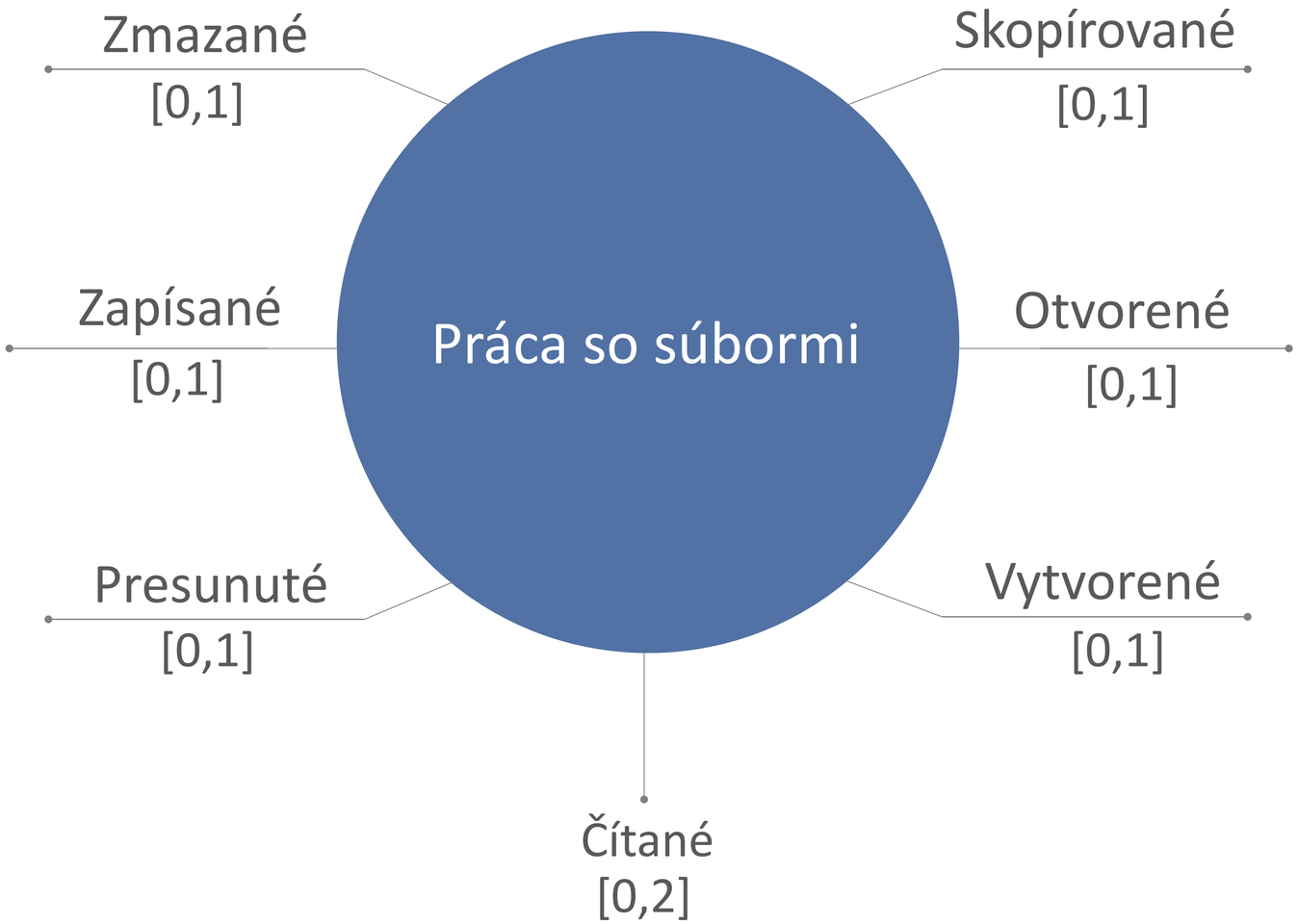
Analýza

- Info
- Signatures
- Network
- Behavior
- Screenshots
- Metadata



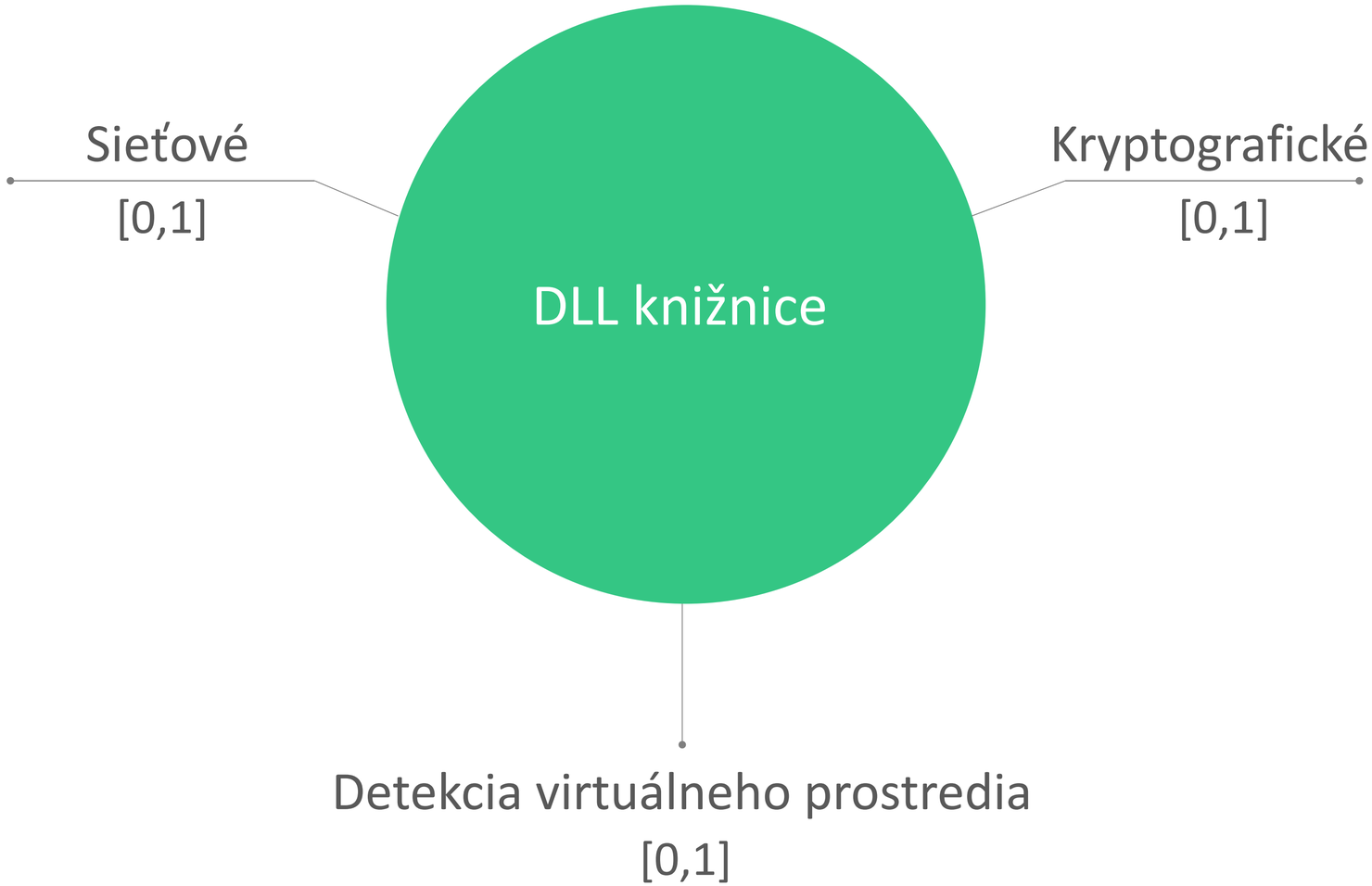
Je to ransomvér?

Behaviorálne atribúty



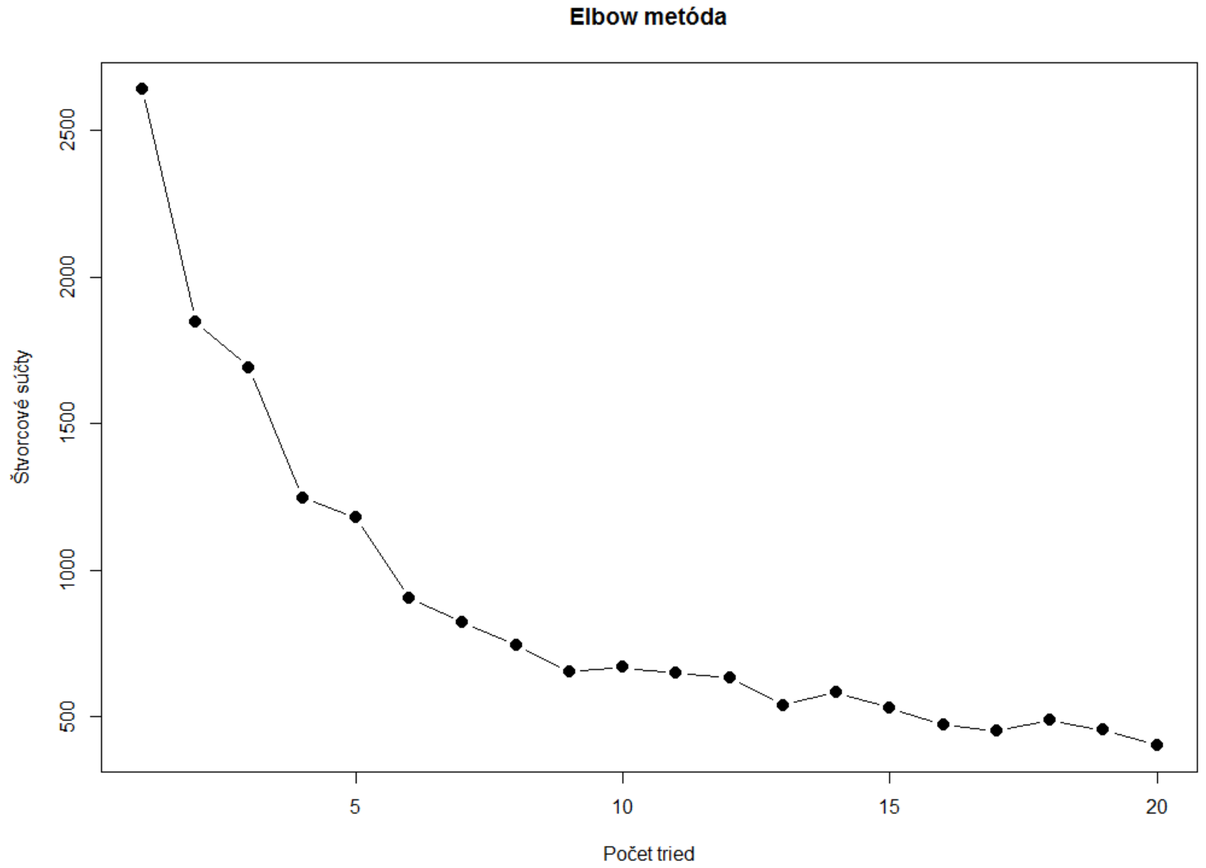
Behaviorálne atribúty

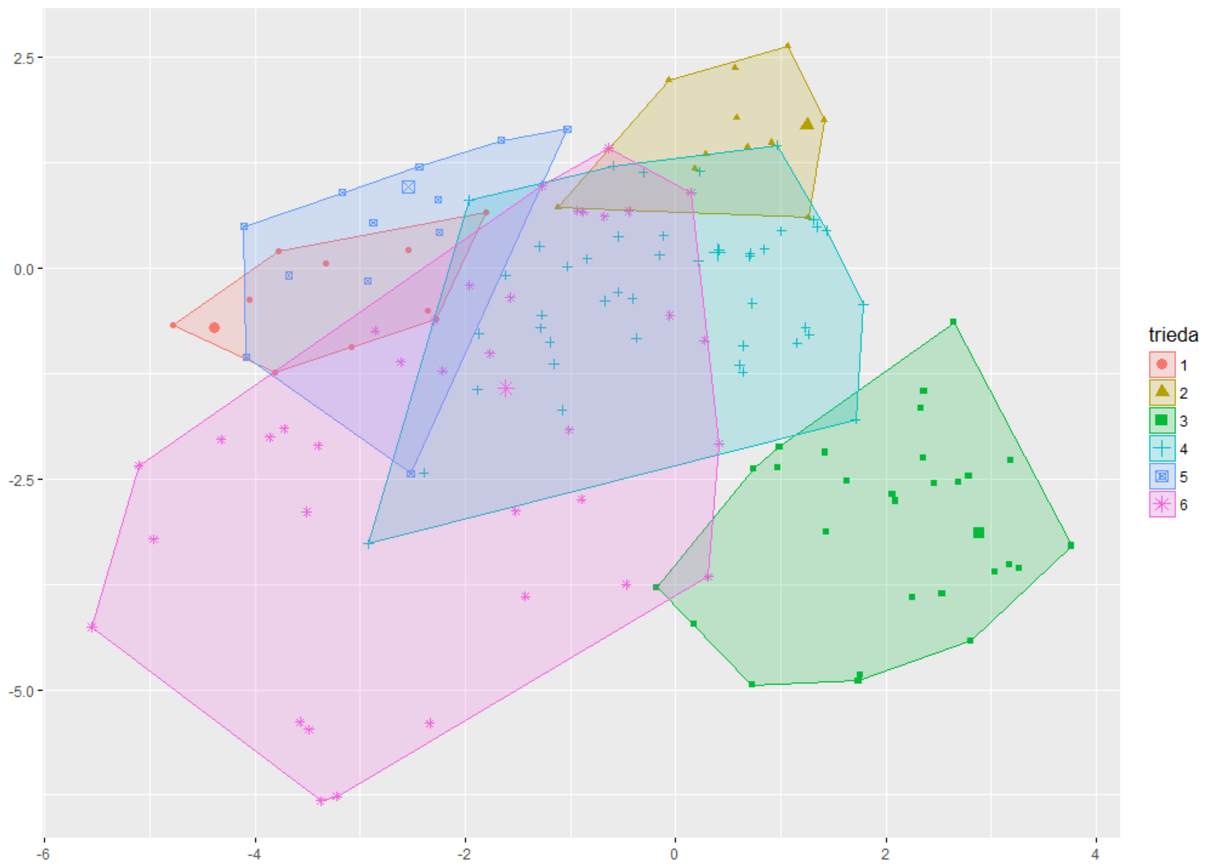
Behaviorálne atribúty



Behaviorálne atribúty

Elbow metóda a K-means algoritmus





Vytvorené triedy

	Práca so súbormi	Výnimky	Sieťová komunikácia			DLL knižnice	Výnimky	Práca s kľúčami v registroch	
			TCP	UDP	DNS			Čítanie	Zapisovanie
1. Trieda	✗	otvorené	✗	✗	✗	✗		✓	✗
2. Trieda	✓		✓	✗	✓	✗	ws2_32, wintrust, cryptsp	✓	△
3. Trieda	✗	čítané	✗	✗	✗	✗		✗	✗
4. Trieda	△ - ✓		△	✗	△	✗	ws2_32, wininet, netapi32	✓	✓
5. Trieda	△ - ✓	presunuté	✗	✗	✗	✗		✓	△
6. Trieda	✓	zmazané, presunuté	✗	✗	✗	✗		✓	△

✗ - (0.0, 0.3]
△ - (0.3, 0.8]
✓ - (0.8, 1.0]

Ďakujem za pozornosť!

Otázky?