Katalóg kryptomien

Jakub Kelečéni
xkelec00@stud.fit.vutbr.cz
Fakulta informačních technológií, Vysoké Učení technické v Brně

ID 21

sMaSheD – Mining Server Detector of Cryptocurrency Pools

1. Úvod a motivácia

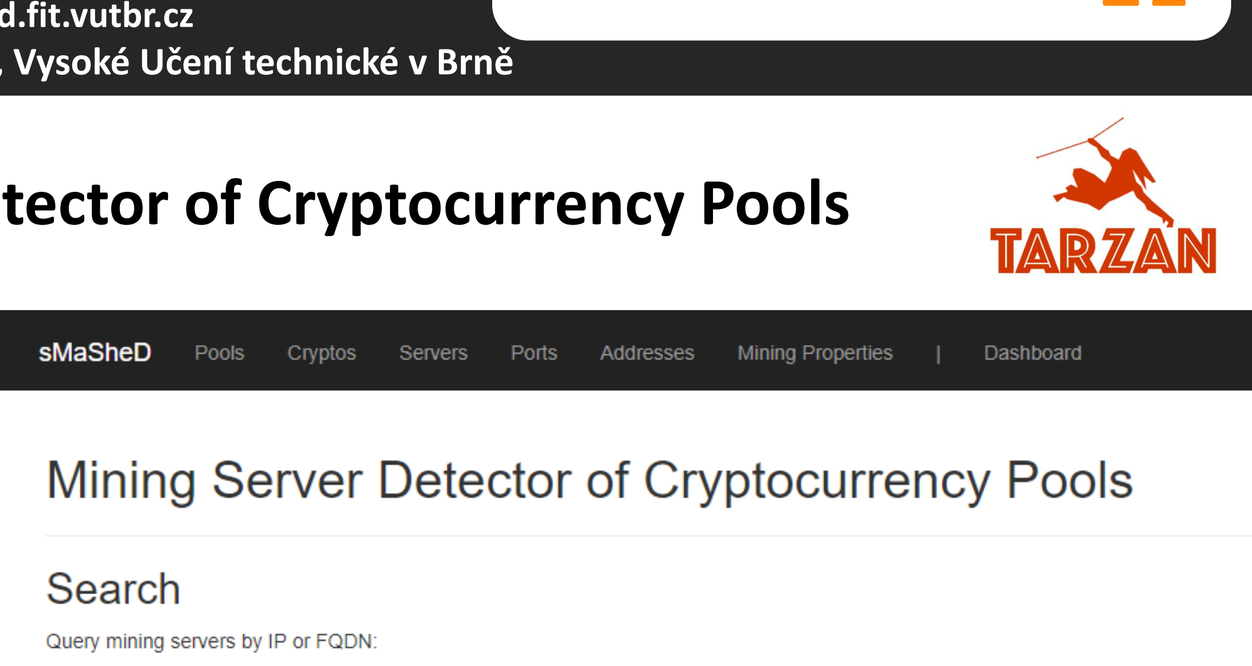
- uchovanie údajov o ťažobných pooloch
  - databáza
  - kryptomeny, pooly, servery, porty
  - detekcia IP adries serverov
  - prehľad uložených informácií

- ciele
  - zdroj dát sieťových administrátorov, bezpečnostné zložky, ...
  - použitie v odbore forenznej analýzy
  - filtrovanie nežiadúcej komunikácie

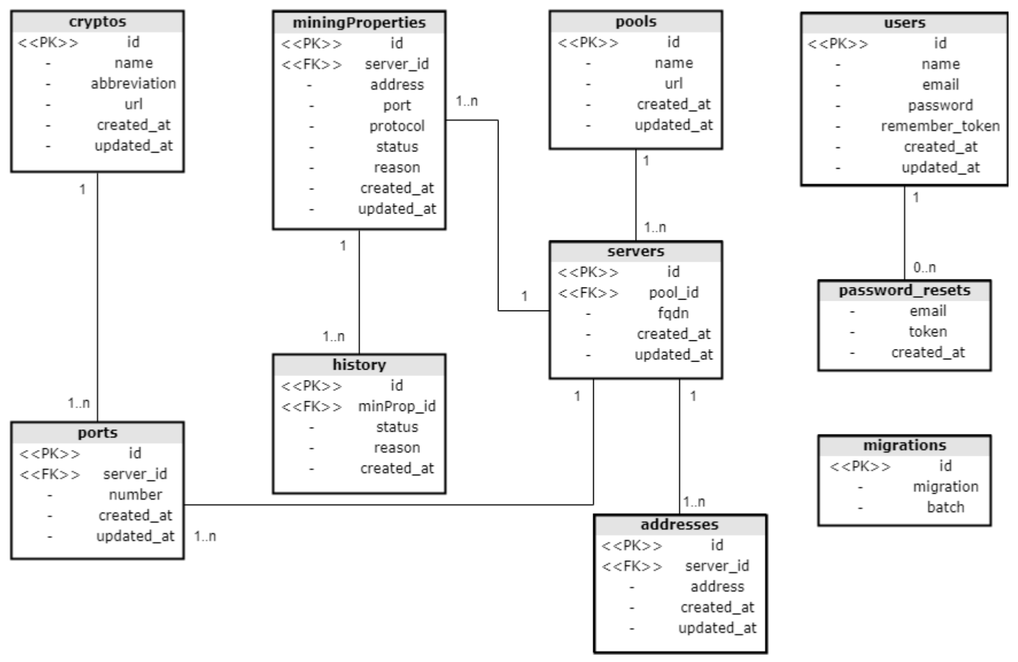
- rozšírenie existujúceho nástroja
  - testovanie dostupnosti ťažobných informácií pre adresu/port v pravidelných intervaloch
  - skutočný stav uložených záznamov

Stav	Kód	Popis
DOWN	0	nedostupná cieľová adresa
UP	1	aktívna implementácia ťažobného protokolu
LISTEN	2	neklasifikovaná odpoveď servera

  - ukladanie histórie dostupnosti



- Databázová schéma nástroja

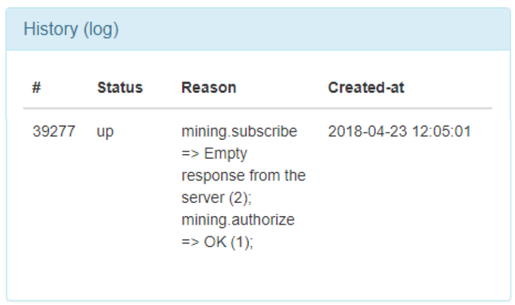


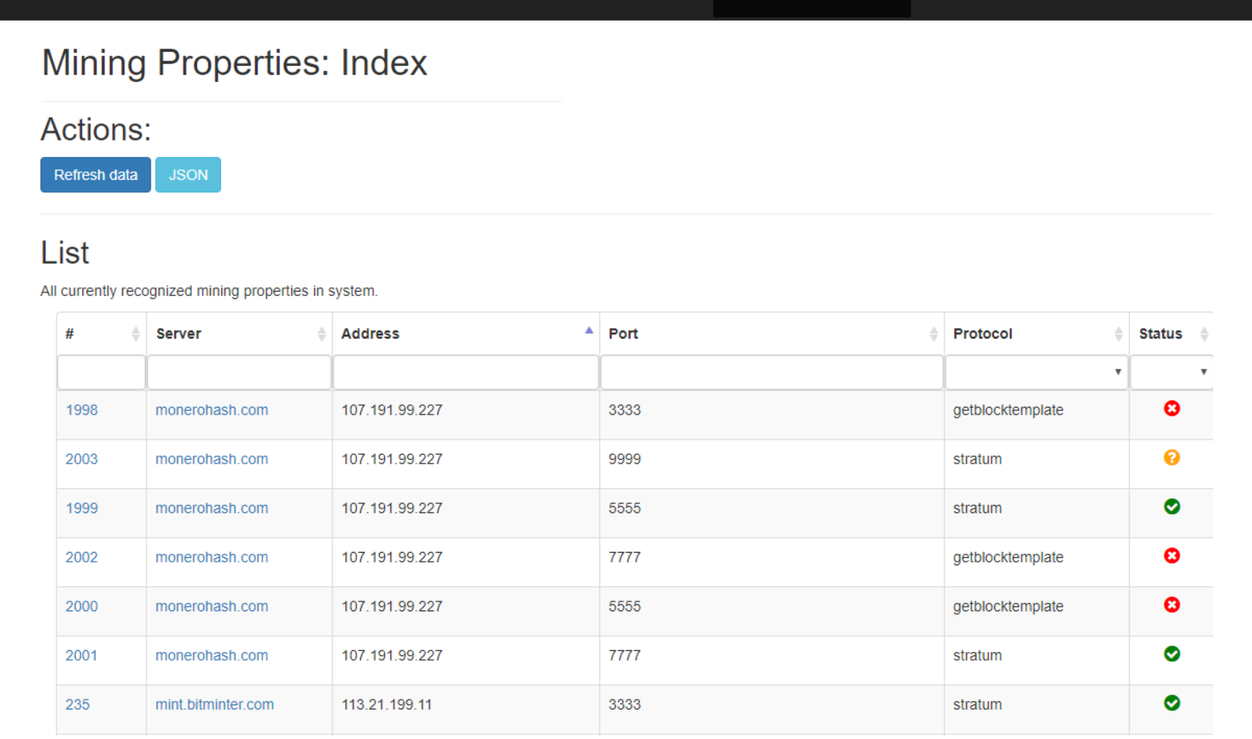
2. Návrh a implementácia rozšírenia

- analýza „ťažobných“ protokolov
  - Getwork (HTTP), Getblocktemplate (HTTP), Stratum (TCP)
  - používané metódy
  - formát a spôsob výmeny správ
    {"jsonrpc": "2.0", "method": "mining.subscribe", "params": ["Miner 1.0"], "id": 1}

- pridanie tabuliek do databáze
  - History
  - MiningProperties

- Pravidelné testovanie uložených záznamov
  - interval 3 hodiny
  - Metódy
    - *mining.subscribe*
    - *mining.authorize*
    - *login*
    - *eth_getwork*
    - *getblocktemplate*
    - *getwork*





- Karta “Mining Properties” – výsledný stav testov

3. Záver

- výsledkom je:
  - doplnenie funkcionality zabezpečujúcej pravidelné testovanie živosti ťažobných poolov
  - dostupnosť uloženého obsahu vo formáte *JSON*
  - lepšia použiteľnosť riešenia ako zdroja dát
    - tvorba pravidiel sieťových filtrov
    - oblasť forenznej analýzy sieťovej prevádzky
  - Stav uložených záznamov
    - 60 % - UP
    - 19 % - LISTEN
    - 21 % - DOWN

- možné rozšírenia:
  - automatické generovanie filtrovacích pravidiel pre sieťové prvky
  - záznam veľkosti hashrate uložených poolov
  - Zahrnutie funkcionality pre správu tzv. multipoolov

- katalóg bol vytvorený v rámci projektu Tarzan
  - Vývoj integrovanej platformy pre spracovanie digitálnych dát z bezpečnostných incidentov