Detekce kryptoměnových těžařů

Jak detekovat Bitcoin minery? Forenzní analýzou provozu!

Technická zpráva projektu TARZAN, FIT VUT v Brně

Vladimír Veselý

Technická zpráva č. FIT-TR-2017-03
Fakulta informačních technologií, Vysoké učení technické v Brně

Naposledy změněno: 12. prosince 2017

Detekce kryptoměnových těžařů

Vladimír Veselý

Vysoké učení technické v Brně, email: veselyv@fit.vutbr.cz

Abstrakt S narůstající popularitou kryptoměn přibývá i případů, kdy dochází k vědomému obohacování těžením bez patřičné refundace a vědomí hostitelské organizace, která těžaři poskytuje zdarma internetové připojení a elektrickou energii. Tato technická zpráva seznamuje čtenáře se všemi detaily procesu těžby kryptoměny a diskutuje možnosti forenzní analýzy nad dostupnými zdroji daty souvisejícími s provozem těžařského hardware i software.

1 Úvod

Motivací kryptoměn je zavedení alternativy k reálným peněžním prostředkům, která není kontrolována vládou (např. centrální bankou). Důvěryhodnost takového elektronického platebního styku spočívá ve využití kryptografických algoritmů k ověření transakcí a spravedlivé emise nových jednotek kryptoměny do oběhu. Dark-web tržiště hojně využívají kryptoměny pro jejich: a) téměř okamžitou a bezplatnou platbu; b) snadno přístupné a změnitelné adresy; c) obtížnou sledovatelnost transakcí (díky broadcastové podstatě šíření informací v peer-to-peer sítích). Několik studií [33], [19], [22] zkoumá Bitcoin jako klíčovou složku jakéhokoli digitálního černého trhu, protože kryptoměny obvykle umožňují zločincům obcházet orgány činné v trestním řízení a regulátory finančního trhu.

Mezi všemi kryptoměnami má Bitcoin [28], [5] výsadní postavení a jeho popularita narůstá od konce roku 2013, kdy začala být jeho nominální hodnota zajímavá pro burzy. Současný (ke měsíci vzniku této práce v srpnu 2017) celkový počet Bitcoins (přibližně 16,5 milionu) představuje více než 71,8 miliardy USD [4]. Bitcoin tvoří peer-to-peer síť s distribuovanou infrastrukturou uživatelů a minerů. Miner ověřuje probíhající transakce za odměnu (buď transakční poplatek nebo nově vydané Bitcoiny). Odměna je vyplácena prvnímu minerovi, který prokazuje transakci tím, že vynakládá svou výpočetní sílu na tento proces. Stejný koncept těžby byl přijat i jinými měnami založenými na systému proof-of-work. Kdokoli se může připojit k sólovému těžebnímu procesu, ale pravděpodobnost, že získá odměnu, bude nízká a riziko zbytečné investované výpočetní síly bez přílišného zisku značné. Proto mineři tvoří tzv. těžební pooly. Když pool získá odměnu, je distribuován provozovatelem poolu mezi minery proporcionálně podle množství jejich vynaložené práce.

Každá organizace by měla monitorovat potenciální existenci minerů (jejich hardwaru i softwaru) ve své síti, a to alespoň z dvou důvodů: a) těžba je často

způsobena malwarem a tak je přítomnost takového zařízení nepřímým indikátorem kompromitace sítě; b) energie (např. elektřina, chlazení, výkon CPU a GPU) vynaložené na těžbu hradí hostitelská organizace, avšak příjemcem odměny není ona sama. Shrnující článek [1] hovoří o různých typech šifrovacích malware určených pro tajnou těžbu na zařízeních - počítačích a serverech, ale také na platformách, jako jsou webové kamery, smartphony nebo síťová úložiště. Typickým příkladem zranitelného prostředí je univerzita, která poskytuje akademickým pracovníkům, vědcům a studentům bezplatné výpočetní prostředky (tj. servery, síť). Uživatel se zlými úmysly může zneužít takové prostředí, což má za následek zvýšenou cenu za elektřinu (např. těžba Bitcoin má vážný dopad na spotřebu elektrické energie [29]), vyčerpané zdroje, ohrožené pracovní procesy a související uživatele.

V tomto článku se zaměřujeme na detekci zařízení, které jsou součástí těžebních poolů. Těžba je aktuálně nejrozšířenějším způsobem, jak mohou účastníci kryptoměnové sítě přijít k novým jednotkám měny.

Navrhujeme dva přístupy, jak detekovat těžaře v síti:

- První přístup je založen na kombinaci pasivního a aktivního sledování provozu. Pasivní monitorování analyzuje záznamy Netflow, zatímco aktivní sledování aktivně sonduje. Pasivní detekce si pomalu vytváří automatizovaně seznam těžebních serverů, což následně snižuje potřebu aktivní detekce. Vzhledem k tomu, že si kdokoli má možnost ad-hoc založit svůj vlastní těžební server či celý pool, tak výsledný seznam veřejně známých těžebních serverů nemůže být považován za úplný. Může se však použít jako vhodný baseline pro detekci minerů jakýmkoli provozovatelem počítačové sítě.
- Druhý přístup může být popsán jako katalog těžebních poolů. Vytvořili jsme veřejně dostupnou webovou aplikaci, která uchovává metadata o stávajících těžebních poolech. Kdokoli má možnost dotazovat se našeho systému, aby zjistil, zda zadané doménové jméno, adresa IP nebo číslo portu je součástí aktuální konfigurace nějakého těžebního poolu.

Tato práce se zaměřuje především na druhý jmenovaný způsob, a proto je zbytek technické zprávy organizován následovně. Část 2 informuje o souvisejících pracích z oblasti kryptoměn. Sekce 3 přináší podrobnosti o aktuální běžné architektuře používané důlní architektuře a zapojených protokolech. Část 4 vysvětluje implementaci a provoz katalogu banských serverů (druhý přístup). Technická zpráva je shrnuta v sekci 5, která také popisuje naši budoucí práci.

2 Současný stav

Tato část shrnuje poznatky z vybraných článků, které se týkají těžby kryptoměn. Snažíme se předložit motivaci pro detekci minerů, poukázat na známé problémy a naznačit výzkumné směry ostatních.

Považujeme Courtois a kol. [10] jako skvělý úvodní zdroj vysvětlující principy těžby Bitcoinů. Autoři poskytují teoretické zázemí, které vysvětluje vazby mezi využívanou kryptografií a těžbou kryptoměny. Tato práce a další, zmíněné

v této části, nám umožňují vynechat důkladný kryptografický popis těžebního procesu. Namísto toho se zaměříme pouze na protokoly a zprávy vyměňované mezi minerem a poolem.

Kroll a kol. [26] a Lawenberg a kol. [27] poskytují ekonomický pohled na těžbu Bitcoinů. Snaží se modelovat proces těžby jako problém s teorií her. Eyal a Sirer [17] diskutují bezpečnost Bitcoinů a motivaci k těžení. Všechny tři články představují i potenciální útoky, které by mohly narušit jakýkoli proces dolování kryptoměny. I my proto zběžně zmíníme "chyby"těžebních protokolů a jejich potenciál k identifikaci minery a jeho korelaci se skutečným uživatelem.

Několik studií [24], [20], [2], [25] uvádí způsoby, jak se kryptoměny dají využít jako monetarizační platforma k protiprávním činnostem. Příklady zahrnují ransomware útoky, command-and-control centra botnetů, krádeže soukromých klíčů, spamové reklamy, podvody typu pay-per-click nebo pay-per-install a další. Náš výzkum doplňuje tyto studie tím, že se zaměřuje na nedovolené těžby kryptoměn.

Huang a kol. [21] poskytuje komplexní studii o typech malwaru, které se zaměřují na pokoutnou těžbu kryptoměn. Autoři vyvinuli metody, které korelují těžebního bota s poolem. Autoři jsou pomocí této metody schopni odhadnout počet infikovaných zařízení, vygenerovaný příjem a trvání botnetové nákazy. Tento dokument považujeme za velkou stimulaci pro naši práci, protože ukazuje, jak úspěšný objev minerů může být rozhodující nejen pro správnou práci v síti, ale také pro významné snížení rizik začlenění zařízení do botnetů. Existuje spojení mezi (neúmyslným) těžením a zneužíváním zdrojů počítačové sítě.

D'Herdt [15] analyzoval zachycené vzorky provozu a navrhl hledat známé porty a adresy IP těžebních serverů. Kromě toho odvodil, že komunikace minerů s důlním serverem není značné, ale často periodická mezi 30-100s. Ačkoli je možné zachytit veškerý síťový provoz i na vysokorychlostním spojení, znamená to, že sledování obrovského množství dat je neúnosné pro dlouhodobé ukládání a poměrně složité pro online analýzu.

Proto se objevily různé agregační přístupy, mimo jiné monitorování průtoku IP reprezentované několika generacemi protokolů NetFlow [8] a IPFIX [3]. Podstatnou charakteristikou při použití flow dat je ztráta informací v porovnání s analýzou kompletně zachyceného toku. Analýza flow je tedy založena na různých heuristikách. Tyto heuristiky (např. použité i pro detekce spamu) vytváří falešně pozitivní výsledky (*false positives*). Je-li počet falešně pozitivních výskytů velmi nízký, heuristiku lze smysluplně použít, v opačném případě (při velkém výskytu falešně pozitivních hlášení) mají síťoví administrátoři tendenci výsledky takových heuristik ignorovat.

3 Architektura Těžby

Tato část poskytuje teoretické zázemí. Vysvětlení celého procesu těžby pro všechny kryptoměny je daleko nad rámec této technické zprávy. Proto jsou zachyceny pouze části týkající se detekce minerů. První podkapitola seznamuje se základní teorii obvyklých operací všech kryptoměn. Druhá podkapitola seznámí čtenáře

s nejmodernějším softwarem a hardwarovým vybavením souvisejících s těžením. Třetí podkapitola poskytuje hlubší popis stávajících těžebních protokolů.

3.1 Teorie

Transakce zapouzdřuje přenos kryptojednotek mezi stranami, kde jedna transakce může obsahovat více vstupů a také výstupů. Chce-li předejít falešným nebo škodlivým transakcím (např. *double-spending problem*), daný uživatel musí ověřit historii transakce. Transakce jsou tedy spojeny dohromady, kde výstupy předchozí transakce slouží jako vstupy další transakce. Transakce za určité období jsou seskupeny do *bloku*, který skupině transakcí dodává zúčtovací čas a kryptografickou integritu. Bloky jsou periodicky zaznamenávány do veřejné účetní knihy přezdívané jako *blockchain*. Bloky jsou spojeny v blockchainu jako jednosměrný vázaný seznam, kde každá položka (tj. blok) má ukazatel na svého předchůdce. Historie každé kryptoměny sahá až k jejímu prvnímu bloku (tzv. *genesis block*), kterým se počíná jejíexistence její a jejího blockchainu. Bloky jsou vytvářeny a jejich obsah ověřován minery (česky též hornicí, havíři, těžaři), kteří vzájemně soutěží (tzv. *mining*, česky též dolování, těžba, ražba) o to, kdo přidá nové bloky do blockchainu. Vítězný miner získává odměnu ve formě nově emitovaných mincí (realizovaných pomocí tzv. *coinbase transakce*). Tyto nově vzniklé mince (jednotky kryptoměny) slouží jako pobídka k dobrovolné účasti na fungování celé peer-to-peer sítě. Vítězem je miner, který by úspěšně vyřešil určitou kryptografickou úlohu (např. výpočet hashe s určitými vlastnostmi na základě vstupu v podobě konstanty plus variabilní nonce) o proměnné složitosti (tzv. *difficulty*, což funguje jako mechanismus zpětné vazby zaručující deterministický čas vytváření bloků). Mineři jsou seskupeni do *poolů*, aby se zvýšila jejich šance na úspěšnou těžbu a tím i odměna v čase.

3.2 Hardware a software

Existuje široká škála různých hardwarových / softwarových nástrojů, které jsou většinou diferencovány na základě použitého hašovacího algoritmu a *hashrate* (což je výpočetní výkon v počtu hashů za sekundu, zkráceně jako hash/s). V závislosti na dané kryptoměně si uživatel zvolí vhodnou kombinaci hardwaru a softwaru, která ovlivňuje proces těžby. Těžební hardwaru ovlivňuje horní mez maximálního možného hashrateu daného uživatele. Výběr těžebního softwaru může optimalizovat a automatizovat proces těžby. Úspěšné zřízení kryptoměnové těžaře se skládá z několika kroků:

1. Volba kryptoměny - Je důležité rozhodnout, jaká kryptoměna bude dolována, protože těžař obykle spekuluje na budoucí cenu. Proto je třeba vzít v úvahu: a) vývoj směnné ceny; b) technologickou životaschopnost měny; c) navyšování složitosti těžby; a d) stále se měnící celkový hashrate celé peer-to-peer sítě. Neexistuje žádná obchodní perspektiva těžby kryptoměny, pokud celkové výdaje převyšují potenciální příjmy. Kvůli velmi volatilním směnným kurzům , je potenciální riziko ztráty neopominutelné, avšak vidina výdělku obvykle příliš lákavá.

2. Výběr poolu - Účast v poolu (ve srovnání se sólovou těžbou) nabízí předvídatelnější generování příjmů, která je úměrná práci vykonávané minerem. Je důležité vybrat si stabilní pool (pokud jde o připojení k internetu a ochranu proti denial-of-service výpadkům) s důvěryhodným provozovatelem poolu (který nefalšuje práci ostatních a férově distribuuje výdělky). Dostupné strategie jakým způsobem jsou odměňováni mineři (např. Pay Per Share, Pay Per Last N Shares, Shared Maximum PPS, Capped Maximum PPS With Recent Backpay) také ovlivňují výběr poolu. Porovnání nejoblíbenějších poolů je k dispozici na následujícím webu [12].
3. Instalace těžebního zařízení - Celková spotřeba energie těžebního hardware jde ruku v ruce s požadavky na elektřinu, chlazení a větrání potřebné k provozu těžby. Takový hardware vyžaduje sice malou šířku pásma, ale neustálé připojení k Internetu, protože si pravidelně vyměňuje pracovní balíčky s těžebním serverem.
4. Konfigurovace těžebního softwaru - Mining pool poskytuje údaje jako IP adresa, doménové jméno, port, podporovaný těžební protokol a TLS/SSL potřebné k úspěšné konfiguraci těžebního software.

Uživatel může ovládat několik zařízení pro těžbu (pracanti též v angličtině *workers*). Každé aktivní těžební zařízení může své pracovním nasazení rotovat klidně mezi několika pooly (např. v režimu load-balancingu, round-robinu či jiné vhodné strategii). Každý těžební hardware je připojen v rámci poolu k jednomu těžebnímu serveru, přičemž přepnutí na sekundární server je v případě výpadku běžnou záležitostí. Spojení mezi horníkem a serverem může být: a) přímé bez proxy (což odhaluje IP adresu minery); b) nepřímé skrz proxy centralizující komunikaci s těžebním serverem, kde proxy může jen přepínat ale dokonce i měnit údaje v těžebním protokolu; c) prostřednictvím overlay sítě ala VPN [1], TOR [2], I2P [3] nebo podobné služby.

Těžba kryptokoměn prodělala následujících pět generačních kroků:

1. CPU těžba - Dolování na procesoru je základní způsob, jak ověřit transakci pro většinu mladých kryptoměn. Tato fáze je možné od chvíle, kdy je známý těžební konsensus (tedy jak ověřovat), ale zatím neexistuje žádná paralelizace této úlohy pomocí jiného hardware. Těžba na klasickém CPU nabízí jen malý hashrate, ale vývoj pro tuto platformu je obvykle nejsnadnější.
2. GPU těžba - Aktuální grafické karty jsou vlastně dedikované superpočítače schopné masivních paralelních výpočtů. GPU má obecně vyšší hashrate než CPU, ovšem jejich efektivita v porovnání s CPU závisí na použitém hashovacím algoritmu (například stejná GPU, které dosahuje při těžbě Bitcoinů hashrate řádově v Mhash/s by Litecoiny těžila v khash/s). Mezi největšími výrobci GPU existuje znatelný rozdíl v hashrate. Karty AMD jsou

[1] Virtual Private Network. Další informace naleznete na adrese https://en.wikipedia.org/wiki/Virtual_private_network

[2] The Onion Router. Další informace naleznete na adrese https://www.torproject.org/

[3] Invisible Internet Project. Další informace naleznete na adrese https://geti2p.net/en/

obecně rychlejší, protože mají lepší podporu aritmetických logických jednotek (ALU) ve srovnání s kartami nVidia, které jsou zaměřeny na operace v jednotce pro výpočty s pohyblivou čárkou (FPU).

3. FPGA těžba - Programovatelná hradlová pole mají mnohem menší spotřebu energie než GPU, ale nárust hashrate není tak velký. FPGA, stejně jako ASICy, jsou navíc k dispozici jen pro omezený počet kryptoměn (a to těch, které skýtají největší obchodní potenciál), protože vývoj a výroba těchto platforem vyžaduje významné investice.

4. ASIC těžba - Aplikačně specifické obvody jsou posledním stupněm hardwarového vývoje těžby. ASIC nabízí nejvyšší možný těžební hashrate a zároveň nejlepší poměr mezi hashrate a spotřebu elektřiny. V současné době ASICy podporují následující hashovací algoritmy doubled SHA-256 [18], Scrypt [32] a X11 [16]. Nicméně ASICy představují hrozbu pro stabilitu jakéhokoli kryptoměnového systému kvůli potenciálně nerovnoměrné distribuci hashrate, kde minorita uživatelů, kteří však vlastní ASICy, obvykle představuje nejsilnější těžební skupinu, což může vést až k teoreticky úspěšnému 51% útoku [9]. Pravděpodobně kvůli podmanivé navratnosti investice je historie výroby ASICů plná příkladů falešných slibů (např. případy ButterflyLabs, Bitmain.ch, CoinTerra) nebo dokonce podvodů (např. případy AlphaTech, BlackArrow). Tudíž jen omezené množství společností je životaschopné v rámci podnikání v tomto odvětví, což vede k postupné monopolizaci trhu; přinejmenším v případě ekosystému Bitcoinů je dominantním výrobcem AntMiner s téměř žádnou konkurencí (tj. Canaan Creative), což platí alespoň v době psaní tohoto článku.

5. Cloudová těžba - Nastartování úspěšné těžební operace vyžaduje netriviální IT znalosti, poprat se s instalací softwaru a investovat do hardwaru. Proto je možnost participovat na těžbě pro většinu obyvatelstva značně komplikovaná. Proto je od roku 2013 stále více populární distanční pronájem těžebního zařízení. Pomocí této služby si zákazník pronajímá těžbní hardware o určitém výkonu na předem omezenou dobu. Vlastníkovi těžebního zařízení je vyplacen nájem po úspěšném ukončení pronájmu. Pronajímatel po dobu nájmu inkasuje vytěžené jednotky nějaké kryptoměny a spekuluje na jejich budoucí cenu. Po dobu trvání nájmu může nájemce dokonce přepnout konfiguraci a začít těžit měnu jinou (pokud tato používá stejný algoritmus hashování). Následující web [11] porovnává různé poskytovatele cloudových služeb.

Pro porovnání generací mezi sebou (a ukázání jejich dopad na fungování ekosystému kryptoměny) použijeme Bitcoin a jeho doubled SHA-256 jako příklad. Vzhledem k tomu, že se těžební technologie rychle vyvíjí, uvádíme v tabulce níže průměrné hodnoty hashrate. Tyto jsou založené na sdílených zkušenostech uživatelů z [6], [7], které byly k dispozici v roce 2013, což byl poslední rok, kdy se všech pět generací těžebních hardware podílelo na fungování Bitcoinu.

Hardware	Generation	Hashrate
Intel i7 Core 3930k	CPU	66 Mhash/s
AMD Radeon 7970	GPU	710 Mhash/s
nVidia GeForce GTX 590	GPU	190 Mhash/s
BitForce SHA256 Single	FPGA	830 Mhash/s
ModMiner Quad	FPGA	800 Mhash/s
ButterFly Labs Single SC	ASIC	30 Ghash/s
Avalon1 A3256 Miner	ASIC	66 Ghash/s

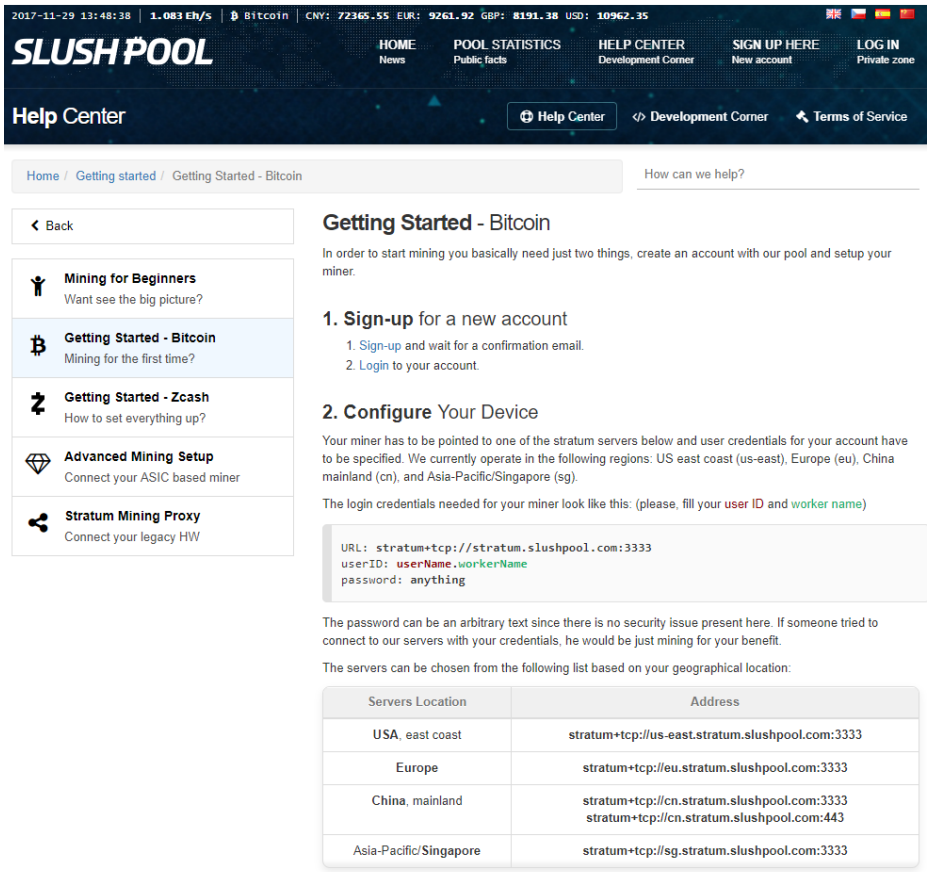
Podle zvolené kryptoměny musí horník instalovat a konfigurovat speciální software, který koordinuje proces těžby mezi těžebním hardwarem a poolem. Úkolem tohoto software je: a) komunikovat s těžebním serverem pomocí těžebního protokolu; a b) předávat hardwaru pracovní balíky ke zpracování. Existuje celá řada způsobů, jak dojíst k těžebnímu konsenzu, které se mezi sebou liší zejména použitým hašovacím algoritmem. Následující tabulka shrnuje některé z existujících softwaru podporujícího těžbu na GPU pro vybrané zástupce kryptoměn:

Cryptocurrency	Algorithm	Mining software
Bitcoin	SHA-256d	cgminer BFGMiner
Litecoin Dogecoin	Scrypt	cgminer BFGMiner
Dash	X11	SGMiner ccMiner
Ethereum Ethereum Classic	Dagger-Hashimoto	ethminer Claymore's Dual Miner
ZCash	Equihash	Silent Army ZCash Miner Claymore's ZCash Miner
Monero	Cryptonight	Wolf Miner ccMiner
Vertcoin	Lyra2RE	SGMiner

Konfigurace těžebního softwaru zahrnuje specifikaci URL či IP adresy těžebního serveru (včetně čísla portu), uživatelské jméno a heslo pro autentizaci minera, nastavení hardwaru (např. preferované GPU kernely, přetaktovávací parametry pro procesor a paměti GPU). Předchozí konfigurační parametry jsou vždy k dispozici na webových stránkách poolu (obvykle i spolu s průvodcem pro začátečníky), aby bylo zajištěno hladké a uživatelsky přívětivé využívání služeb poolu.

3.3 Protokoly

Pool a jeho členové využívají speciální komunikační protokoly pro koordinaci a distribuci těžebního procesu. Aktuálně existují tři těžební protokoly podporované většinou kryptoměn:



Obrázek 1: Ukázka z webu SlushPool obsahující pokyny k základnímu nastevní těžebního software

– *GetWork* byl navržen jako první těžební protokol. Ve srovnání se svými následníky je GetWork poměrně jednoduchý protokol a odpovídá schématu, kde těžební server přiřadí pracovní balíček a miner slepě provádí proces ověřování transakce. Díky své přílišné jednoduchosti umožňuje GetWork podvratnému operátorovi poolu realizovat korektní ověření double-spent transakcí. Zprávy protokolu GetWork jsou zakódovány v JSON [4] syntaxi nesené uvnitř protokolu HTTP [5]. GetWork podporuje jen omezené množství rozšíření nad rámec úvodní protokolové specifikace, a to při použití dodatečných HTTP hlaviček.

[4] JavaScript Object Notation. Další informace naleznete v https://tools.ietf.org/html/rfc7159

[5] Hypertext Transfer Protocol. Další informace naleznete na adrese https://tools.ietf.org/html/rfc7230

– *GetBlockTemplate* je oficiální protokol k těžbě vyvinutý v rámci Bitcoinovy komunity, ale přijatý i jinými kryptoměnami. GetBlockTemplate byl kodifikován v BIP [6] 22 [13]. GetBlockTemplate nabízí větší decentralizaci tím, že proces vytváření bloků se děje na minerech a nikoli na těžebním serveru. GetBlockTemplate zvyšuje maximální velikost pracovního balíčku a snižuje režii těžebního protokolu, což je v souladu s existencí ASICů, pro které je GetWork příliš těžkopádný. Navíc BIP 23 [14] standardizuje rozšíření a způsoby, jak flexibilně vylepšit GetBlockTemplate bez jakéhokoli významnějšího redesignu samotného protokolu a bez použití nekonformních HTTP hlaviček.
– *Stratum* protokol [30] byl prototypován M. Palatinusem, vynálezcem koncepce poolové těžby a provozovatelem nejstaršího Slush poolu [31]. Vývoj protokolu Stratum byl motivován potřebou odstranit návrhové chyby předchozích dvou protokolů, a to: a) oprostěním se od HTTP jako nosného protokolu pro zprávy, což snižuje nadbytečnou režii; b) zbavením se tzv. long-pollingu, který je neškálovatelný; a c) přidáním extranonce políčka, které umožňuje minerovi vygenerovat si více hashů lokálně, aniž by obtěžoval těžební server požadujíce nový pracovní balíček. Stratum je kompatibilní s JSON-RPC 2.0 [23] a pracuje přímo nad protokolem TCP.

Všechny výše zmíněné protokoly využívají protokol TCP [7] jako protokol transportní vrstvy. Ve srovnání s oficiálními klienty, kteří se připojují k peer-to-peer síti dané kryptoměn, těžební protokoly nepoužívají žádné well-known číslo portu. Záleží pouze na preferenci správce poolu, na kterém porty naslouchají jeho servery. Často se využívá portů 80, 443 a 25, protože nejsou obvykle blokované na žádných firewallech.

Obvyklá výměna zpráv zahrnuje několik kroků. S počáteční zprávou se miner připojuje k těžebnímu serveru a poskytuje autentizacční údaje. Autentifikace je nutná, protože na základě nich pool ví, na jaký účet průběžně připisovat dílčí odměny za odevedenou práci. Dvě typy ověřování jsou běžné:

– *registrační* - Před zapojením se do poolu musí majitel težebních zařízení provést registraci svého účtu. Součástí správy účtu je i správa pracovníků. Autentifikace vůči poolu se pak provádí na základě známého uživatelského jména.
– *bezregistrační* - Některé pooly nabízejí své služby bez jakékoli registrace účtu. V takovém případě obvykle miner poskytuje pouze svou kryptoadresu jako uživatelské jméno pro ověření, na níž pak pool zasílá odměny.

Nezávisle na typu autentizace může uživatelské jméno obsahovat volitelné přípony, jako je identifikátor pracovníka (s cílem rozlišit různé pracovníky stejného uživatele) nebo e-mailovou adresu (kde je uživatel informován o jakýchkoli problémech zjištěných při těžbě).

[6] Bitcoin Improvement Proposal. Viz https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki

[7] Transmission Control Protocol. Další informace naleznete na adrese https://tools.ietf.org/html/rfc793

Dalším krokem při komunikaci s těžebním protokolem je opakované přidělování pracovních balíčků poskytovaných serverem. Každý pracovní balíček obsahuje *data*, *target* a *nonce* (ostatní pole závisí na kryptoměně). Miner se pokusí nalézt hash (kombinováním dat a nonce), který splňuje (tj. jeho binární hodnota je nižší než) cíl. Různé kryptoměny používají odlišné hashovací algoritmy - např. SHA-256d pro Bitcoin, Scrypt pro Litecoin, X11 pro Dash. Miner buď předloží správné řešení nebo pokračuje v práci na jiném pracovním balíčku.

Obrázek 2: Example of Stratum protocol message exchange

Výše uvedený obrázek znázorňuje Stratum komunikaci mezi minerem (červená barva) a jeho serverem (modrá barva). Můžeme pozorovat typickou výměnu zpráv. Připojení k poolu je iniciováno první zprávou (označenou jako #1), kde můžeme vidět podrobnosti o autentizaci. Server potvrzuje zprávou označenou jako #2. Server odešle pracovní balíček (#3), který je třeba zpracovat. Po správné inicializaci těžebního softwaru požádá miner o nový pracovní balíček (#4), který poskytuje server (# 5). Miner úspěšně vyhledá hash a předloží kompletní řešení (#6) zpět na server. Server rozhoduje o tom, zda je výsledok těžby platný nebo neplatný. V případě #7 je platný, a tak zašle nový pracovní balíček (#8). Miner začne zpracovávat nový balíček a mezitím pravidelně informuje server o jeho aktuální výpočetní rychlosti (zpráva označená jako #9) tak, aby server mohl dynamicky upravit velikost následujících pracovních balíčků.

Pokud se zaměříme na forenzní analýzu metadat týkajících se důlního protokolu, pak můžeme extrahovat:

– IP adresy a čísla portů - Kontrolami adres IP lze geolokovat jak minera, tak těžební server. Spolu s čísly portů můžeme účtovat síťový provoz pomocí služby NetFlow. Jakmile máme k dispozici záznamy NetFlow, můžeme odpovědět na otázky, jako např. jak dlouho byl miner aktivní, kolik těžebních zařízení je v naší síti připojeno, apod.

– Informace o poolu - rozšíření protokolů GetWork nebo GetBlockTemplate mohou odhalit další užitečné informace, jako jsou alternativní banské servery včetně jejich adres IP, plně kvalifikovaných doménových jmen a čísel portů.
– Uživatelské jméno - Na základě typu autentizace může pole uživatelského jména obsahovat buď přezdívku nebo název účtu uživatele fondu nebo jeho adresu kryptosměn. Tyto informace mohou být rozhodující pro úspěšnou korelaci skutečného člověka a jeho elektronické identity.
– Heslo - Autentizační zpráva jakéhokoliv důlního protokolu obsahuje heslo. Nicméně je zřídkakdy využíváno pro autorizaci nebo pro jakýkoli účel skupinou. Výchozí hodnota pole pro heslo pro většinu důlního softwaru je 'x'.
– E-mailová addresa - Některé fondy nabízejí e-mailové upozornění o postupu hornické činnosti. V případě jakéhokoli problému, jako je výpadek horníků, příliš mnoho odmítnutých akcí nebo odpojení od bazénu, je uživatel upozorněn e-mailem. E-mailová adresa může být volitelně součástí podadresářské zprávy, která může pomoci odhalit totožnost uživatele.

Během fáze zkoumání detekčních metod minerů jsme potřebovali relevantní data. Proto jsme si vytvořili vlastní datasety obsahující pakety, které se vyměňované našimi zkušební mineři se servery různých poolů těžíce různé kryptoměny. Tyto datasety jsou veřejně k dispozici každému, kdo by měl zájem o následný výzkum týkající se protokolů o těžbě.

4 Katalog kryptoměny

V teto kapitole je stručně popsán systém sMaSheD, aneb *Mining Server Detector*. Jedná se o webovou aplikaci s responzivním uživatelským rozhraním, která umožňuje návštěvníkovi zodpovědět jednoduchý dotaz, a to jestli danou IP adresu či doménové jméno volitelně i s portem systém eviduje jako známý server přidružený k nějakému těžebnímu poolu.

V době psaní této práce je systém sMaSheD dostupný veřejně na IP odkaze http://147.229.9.85.

4.1 Implementační detaily

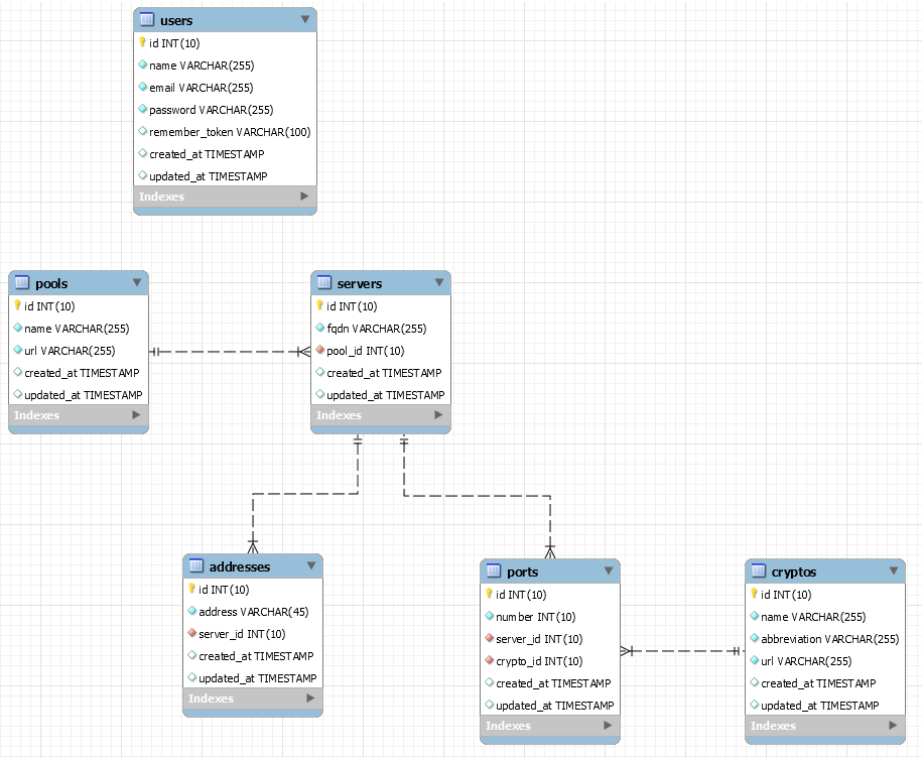
O webovou komunikaci se stará Apache 2.4.18. Systém je implementován v jazyce PHP 7.0, a to nad frameworkem Laravel 5.4. Vizuální stránka webu vyúžívá knihovny Boostrap 3.0. Persistetní data jsou skladována v databázi MySQL (s démonem ve verzi 14.14).

Databáze využívá následující schéma:

Z pohledu systému sMaSheD jsou důležité tabulky: *pools*, *servers*, *addresses*, *ports* a *cryptos*. Kromě nich se vyskytují ještě provozní tabulky Laravel frameworku *migrations* a *password-resets*.

Platí, že:

1. 1 pool má N serverů
2. 1 server má N adres IPv4 či IPv6
3. 1 adresa má N portů
4. K danému 1 portu patří 1 kryptoměna



Obrázek 3: Relační schéma databáze

4.2 Přehled funkce

V této sekci je předvedena ukázková funkcionalita, kterou systém sMaSheD disponuje a nabízí svým uživatelům.

Hlavní stránka Na úvodní obrazovce ?? lze do vyhledávacího políčka vložit IP adresu či FQDN a volitelně dodat i port. Systém projde existující obsah databáze a pokusí se najít odpovídající záznam. Ke známému serveru jsou zobrazeny patřičné informace.

Dashboard Obrazovka dashboardu ?? shrnuje základní informace o systému - kolik registruje poolů, serverů, adres a kryptoměn.

Entity Pro každou tabulku v systému je vytvořena dedikovaná webovka, skrz kterou si lze vylistovat všechny záznamy. Navíc po úspěšné autentizaci uživatele vůči systému lze záznamy přidávat, editovat a mazat. Následující obrazovka ?? demonstruje jednoduchost přidávání nového serveru.

5 Závěr

Tato technická zpráva popisuje principy kryptoměnové těžby a forenzně-analytický potenciál této operace. Cílem této technické zprávy je podat základní informace o těžbě čtenáři s žádnými, nebo malými informacemi o kryptoměnách jako takových. Technická zpráva může sloužit také jako rozcestník k dalším zdrojům dostupných na webu i ve vědeckých publikacích.

Odkazy

[1] Syed Taha Ali, Dylan Clarke a Patrick McCorry. „Bitcoin: Perils of an unregulated global p2p currency“. In: *Cambridge International Workshop on Security Protocols*. Springer. 2015, s. 283–293.

[2] Syed Taha Ali et al. „ZombieCoin: powering next-generation botnets with bitcoin“. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2015, s. 34–48.

[3] P. Aitken B. Claise B. Trammell. *Specification of the IP Flow Information Export (IPFIX) Protocol*. RFC 7011. IETF, zář. 2013, s. 1–75. URL: %5Curl%7Bhttps://tools.ietf.org/html/rfc7011%7D.

[4] *Bitcoin (BTC) | CryptoCurrency Market Capitalizations*. https://coinmarketcap.com/currencies/bitcoin. Accessed: 2017-05-30.

[5] *Bitcoin - Open source P2P money*. https://bitcoin.org/en. Accessed: 2017-05-30.

[6] Bitcoin.it. *Mining hardware comparison - Bitcoin Wiki*. https://en.bitcoin.it/wiki/Mining_hardware_comparison. Accessed: 2017-08-24.

[7] Bitcoin.it. *Non-specialized hardware comparison*. https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison. Accessed: 2017-08-24.

[8] B. Claise. *Cisco Systems NetFlow Services Export Version 9*. RFC 3954. IETF, říj. 2004, s. 1–32. URL: %5Curl%7Bhttps://tools.ietf.org/html/rfc3954%7D.

[9] CoinDesk. *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*. https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/. Accessed: 2017-08-24.

[10] Nicolas T Courtois, Marek Grajek a Rahul Naik. „The unreasonable fundamental incertitudes behind bitcoin mining“. In: *arXiv preprint arXiv:1310.7935* (2013).

[11] CryptoCompare. *Compare Bitcoin, Ethereum and Litecoin Mining Contracts*. https://www.cryptocompare.com/mining/#/contracts. Accessed: 2017-08-24.

[12] CryptoCompare. *Compare Bitcoin, Ethereum and Litecoin Mining Pools*. https://www.cryptocompare.com/mining/#/pools. Accessed: 2017-08-25.

[13] Luke Dashjr. *getblocktemplate - Fundamentals*. BIP 22. Bitcoin Project, ún. 2012. URL: %5Curl%7Bhttps://github.com/bitcoin/bips/blob/master/bip-0022.mediawiki%7D.

[14] Luke Dashjr. *getblocktemplate - Pooled Mining*. BIP 23. Bitcoin Project, ún. 2012. URL: %5Curl%7Bhttps://github.com/bitcoin/bips/blob/master/bip-0023.mediawiki%7D.

[15] Jan D'Herdt. *Detecting Crypto Currency Mining in Corporate*. Tech. zpr. SANS Institute, led. 2015.

[16] E. Duffield, D. Diaz. *Dash: A Privacy-Centric Crypto-Currency*. Tech. zpr. Břez. 2017. URL: %5Curl%7Bhttps://github.com/dashpay/dash/wiki/Whitepaper%7D.

[17] Ittay Eyal a Emin Gün Sirer. „Majority is not enough: Bitcoin mining is vulnerable“. In: *International conference on financial cryptography and data security*. Springer. 2014, s. 436–454.

[18] Quynh H. Dang. *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication FIPS Pub 180-4. Břez. 2012, s. 30. URL: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

[19] Reuben Grinberg. „Bitcoin: An Innovative Alternative Digital Currency"(2012)“. In: *Hastings Sci & Tech LJ* 4 (), s. 159–208.

[20] Nikolai Hampton a Zubair A Baig. „Ransomware: Emergence of the cyber-extortion menace“. In: (2015).

[21] Danny Yuxing Huang et al. „Botcoin: Monetizing Stolen Cycles.“ In: *Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS)*. 2014, s. 16. DOI: https://doi.org/10.14722/ndss.2014.23044.

[22] Beverly Johnson. „The advantages and disadvantages of the Deep Web, Tor network, virtual currencies and the regulatory challenges thereof“. Dipl. USA: Utica College, 2014.

[23] JSON-RPC Working Group. *JSON-RPC 2.0 Specification*. http://www.jsonrpc.org/specification. Accessed: 2017-08-17. 2017.

[24] Ari Juels, Ahmed Kosba a Elaine Shi. „The ring of Gyges: Investigating the future of criminal smart contracts“. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, s. 283–295.

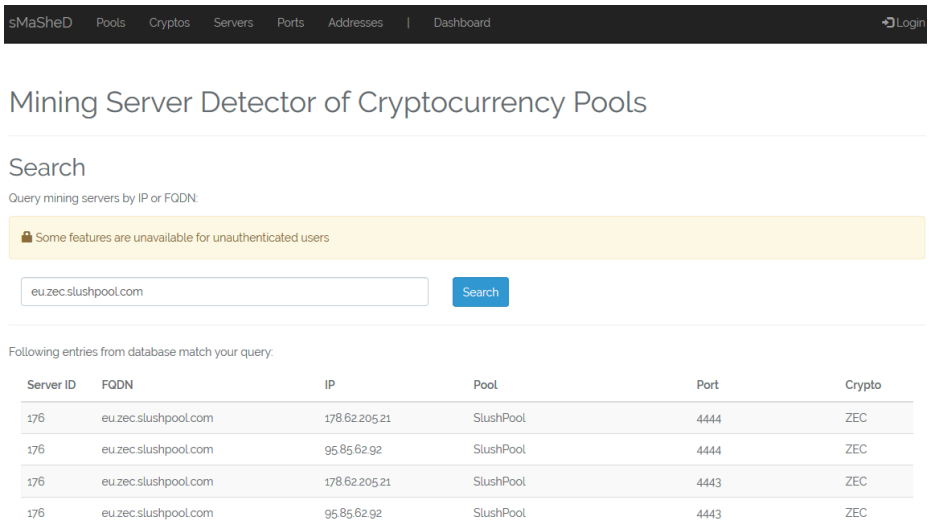
[25] Amin Kharraz et al. „Cutting the gordian knot: A look under the hood of ransomware attacks“. In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer. 2015, s. 3–24.

[26] Joshua A Kroll, Ian C Davey a Edward W Felten. „The economics of Bitcoin mining, or Bitcoin in the presence of adversaries“. In: *Proceedings of WEIS*. Sv. 2013. 2013.

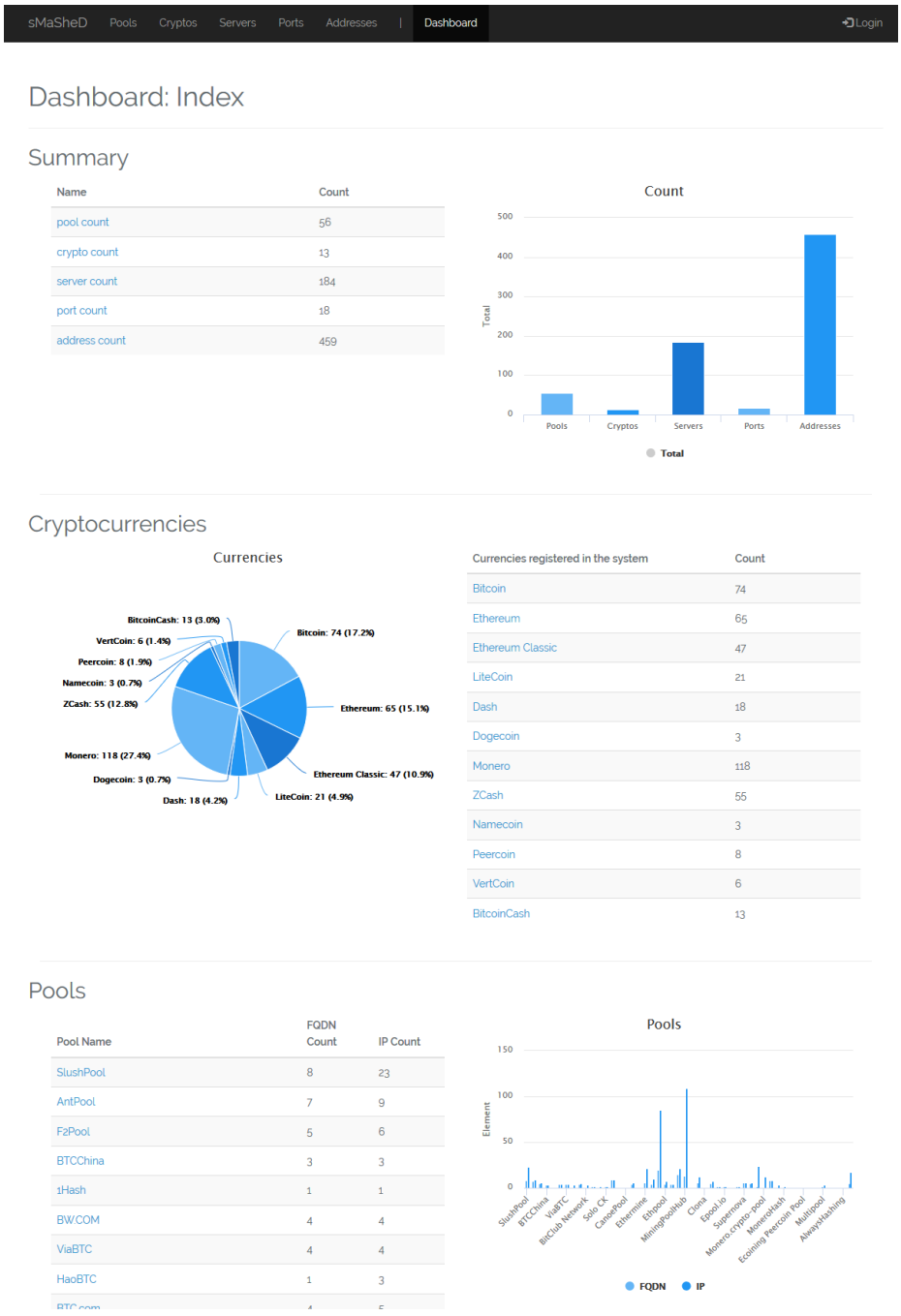
[27] Yoad Lewenberg et al. „Bitcoin mining pools: A cooperative game theoretic analysis“. In: *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International

Foundation for Autonomous Agents a Multiagent Systems. 2015, s. 919–927.
[28] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Accessed: 2017-05-30.
[29] KJ O'Dwyer a D Malone. „Bitcoin Mining and its Energy Footprint". In: *IET Conference Proceedings*. The Institution of Engineering & Technology. 2014.
[30] Marek Palatinus. *Help Center – slushpool.com*. https://slushpool.com/help/manual/stratum-protocol. Accessed: 2017-08-17. 2017.
[31] Marek Palatinus. *Homepage – slushpool.com*. https://slushpool.com/help/manual/stratum-protocol. Accessed: 2017-08-17. 2017.
[32] Colin Percival a Simon Josefsson. *The scrypt Password-Based Key Derivation Function*. RFC 7914. Srp. 2016. DOI: 10.17487/RFC7914. URL: https://rfc-editor.org/rfc/rfc7914.txt.
[33] Reza Raeesi. „The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?" In: *Glendon Journal of International Studies/Revue d'études internationales de Glendon* 8.1-2 (2015), s. 20. DOI: \url{http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.960.6973}.

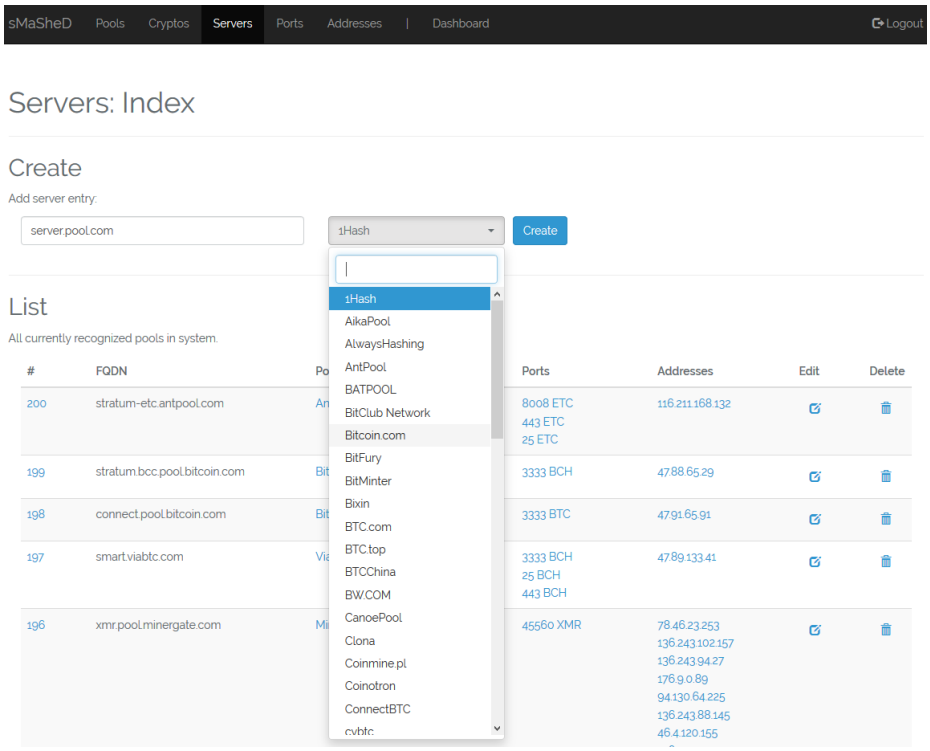
A Obrazovky systému sMaSheD



Obrázek 4: Pokusné vyhledání serveru eu.zec.slushpool.com



Obrázek 5: Stav dashboardu k prosinci 2017



Obrázek 6: Přidávátko nového serveru