do whoisu, jako je tomu u standardních domén ve správě ICANN, a jedinou informaci, kterou o doméně najdeme, je namecoinová peněženka, ze které bylo za vytvoření či úpravu záznamu zaplaceno.

Samotná transakce nemá příjemce, kterému by se za doménu platilo – dochází totiž k úplnému odstranění utracených namecoinů.

Registrovat doménu je možné skrze open source klienta vytvořeného vývojáři namecoinu nebo skrz třetí stranu – registrátory (např. peername.com či dotbit.me), což ovšem může snížit míru anonymity a být mnohonásobně dražší. Registrace domény přímo přes namecoin klienta vychází zhruba na jednu korunu.

Jeden zásadní problém s doménami .bit je fakt, že nepatří do standardního doménového systému a systémy je zpravidla neumějí ve výchozím nastavení přeložit. Možností, jak překládat .bit domény, je více:

- Použití OpenNIC DNS serverů. Jde o alternativní doménový systém, který umožňuje kromě překladu standardních domén také celou řadu jiných alternativních domén jako například .bbs, .chan a další (také neoficiální národní domény jako .ku pro kurdské či .ti pro tibetské weby).

OpenNIC spolupracuje také s namecoinem a v pravidelných intervalech zpracovává záznamy z namecoin blockchainu do formy DNS zóny a propaguje ji do svých (komunitně provozovaných) DNS serverů, skrze které je pak možné doménu přeložit.

- Provozování vlastního DNS serveru za použití softwaru ncdns, který bude zcela nezávislý na provozovatelích třetích stran a data bude získávat přímo z blockchainu.
- Instalací doplňku do prohlížeče, který zpřístupní stránky z alternativních doménových systémů.

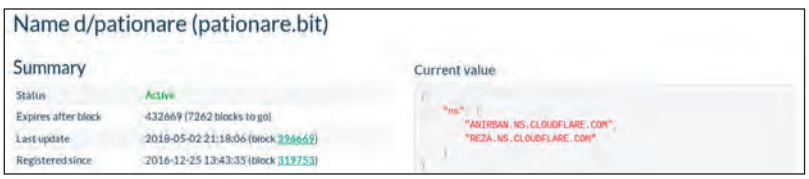
Malware na .bit

Asi nikoho nepřekvapí, že vlastnost decentralizace a relativní anonymity je atraktivní právě i pro tvůrce malwaru, a v posledních letech tak roste využívání, resp. zneužívání těchto domén. Je to způsob, kterým se mohou tvůrci malwaru elegantně vyhnout zmíněným rizikům, která hrozí v případě použití standardních domén.

Jediný způsob, jak by orgány činné v trestním řízení mohly proti doméně zakročit, je odstavení celého blockchainu, což je v podstatě neproveditelné a poškodilo by to i všechny legitimní uživatele.

Ukázkou může být doména pationare.bit fungující od prosince 2016, za kterou údajně běžel řídící server bankovního trojského koně Chthonic. Ten byl v polovině roku 2017 analyzován, nicméně rok 2018 se blíží ke konci a doména je stále aktivní. *(Viz obrázek.)*

Blockchain má na druhou stranu pro útočníka také nevýhodu – záznamy jsou v něm veřejně přístupné, a to i historické. Veškeré informace, které kdy útočník vloží k dané doméně, již není možné odstranit, a dají se v nich tak hledat spojitosti.



[Z pohledu obrany je na zvážení, zda není řešením kompletní blokace všech .bit domén v síti, pokud to neuškodí běžnému provozu.]

Průzkum blockchainu je možný například na stránkách namecha.in. Něco takového není v tradičním doménovém světě možné, ke zpětným údajům o doménách se nelze běžně dostat, pouze částečnou výjimku tvoří systémy Passive DNS, které se snaží historii domén zachytávat.

Zmíněná nutnost upravit DNS nastavení pro překlad .bit domén je z pohledu útočníka výhodou i nevýhodou.

Výhodou proto, že ztěžuje analýzu vzorku takového malwaru a také se snáze vyhne různým automatickým reputačním systémům, které doménu nepřeloží a z jejich pohledu bude doména vypadat mimo provoz, takže systém ani nezaznamená žádný závadný obsah.

Nevýhodou pak proto, že jde o kritický bod pro funkcionalitu malwaru, a pokud by se odřízl, útočník může přijít o kontrolu nad nakaženým strojem. Identifikovat změnu DNS nastavení v systému, kterou by malware mohl vykonat, není pro administrátora náročné.

To však lze obejít například použitím nezdokumentované části Windows API, přes které je možné nastavit DNS server pro překlad každého individuálního požadavku, a není třeba měnit systémové nastavení.

V případě, kdy se tvůrce malwaru rozhodne využít překlad skrze komunitně provozované OpenNIC servery, je také rizikem jejich dostupnost, neboť je provozují nadšenci a dobrovolníci, u kterých není žádná záruka nepřetržitého provozu.

Z pohledu obrany je tak na zvážení, zda v tom či onom konkrétním případě není řešením kompletní blokace všech .bit domén (či jiných alternativních domén) v síti, pokud to neuškodí běžnému provozu.

Útočníci mají ve svém repertoáru pro obfuskaci infrastruktury jejich botnetu i další techniky, jako jsou třeba fast-flux, algoritmické generování domén (DGA) či využití Toru. Blockchainové domény se tak zařazují do tohoto repertoáru a dá se očekávat, že v budoucnu se budou v různých kombinacích objevovat stále častěji. ■

Vznik tohoto textu byl podpořen Nástrojem Evropské unie pro propojení Evropy.
Autor je bezpečnostní analytik sdružení CZ.NIC