Nezlomná doména, která využívá blockchain

Botnety dostávají do rukou mocný nástroj, který je může ochránit před případným zablokováním – jsou jimi tzv. blockchainové domény.

FILIP POKORNÝ

Malware v dnešní době se zpravidla snaží komunikovat se svým řídícím serverem (command & control), na který jednak zasílá získané informace a naopak od něj dostává instrukce, co dál dělat. Tato komunikace je jedním z článků, na který se bezpečnostní pracovníci často zaměřují a snaží se ho přerušit.

Nejčastějším způsobem, jak to učinit, je odstranění nebo zablokování těchto řídících serverů. Toho jsou si tvůrci malwaru samozřejmě vědomi, a tak do kódu malwaru nevkládají „natvrdo" napsané IP adresy řídících serverů, ale raději domény.

To poskytuje malwaru větší odolnost, neboť v případě zablokování IP adresy serveru, na kterou doména odkazuje, stačí útočníkovi upravit DNS záznam domény na IP adresu jiného řídícího serveru.

Ovšem ani tento způsob není neprůstřelný, protože běžné domény se spravují centralizovaně různými registry, podléhají pravidlům ICANN (Internet Corporation for Assigned Names and Numbers, nezisková organizace pro přidělování a správu doménových jmen a IP adres) a jsou registrované skrze registrátory.

[Vlastnost decentralizace a relativní anonymity je pro tvůrce malwaru atraktivní, a v posledních letech tak roste využívání, resp. zneužívání blockchainových domén.]

Registry či registrátoři pak mohou spolupracovat s bezpečnostními výzkumníky nebo musejí vyhovět například žádostem orgánů činných v trestním řízení, a doménu tak zrušit, pozastavit nebo i přesměrovat (sinkhole).

Útočník tím ztrácí možnost komunikovat s kompromitovanými stroji (boty), a kontrolovat tak svůj botnet. Proto přicházejí tvůrci malwaru stále s novými důmyslnými způsoby, jak vytvořit dostatečně houževnatou infrastrukturu botnetu, která by co nejdéle odolávala snahám o její narušení.

Doména .bit

V roce 2011 vznikla po vzoru bitcoinu decentralizovaná kryptoměna Namecoin. Ta umožňuje v rámci blockchainu uchovávat další data jako například DNS záznamy pro domény .bit. Vzhledem k decentralizované povaze je nemožné takovou doménu odstranit třetí stranou.

Navíc je značně anonymní, protože pro její registraci není třeba uvádět vlastníka či jiné kontaktní údaje