Vážené čtenářky, vážení čtenáři,

poslední dobou je nejskloňovanější hrozbou pro počítače těžba kryptoměn. Samozřejmě nikoliv ta, kterou si tito dobrodruzi vykonávají na vlastních počítačových systémech. Řeč je o podvodnících, jež se snaží využít cizí výpočetní zařízení k tomu, aby práci udělala za ně.

Cryptojacking, jak se tato činnost nazývá, má podobný vektor šíření jako ransomware včetně taktiky nakažených webových stránek nebo škodlivého odkazu v e-mailové zprávě. Oběť nevědomky načte šifrovaný kód pro těžbu kryptoměny nebo z webu stáhne nakažený JavaScript mající navenek například formu nějaké reklamy, který se následně spustí v prohlížeči zasaženého počítače.

Na rozdíl od ransomwaru se však cryptojacking snaží být v hostitelském počítači co nejméně nápadný, protože čím déle pro něj napadený počítač bude pracovat, tím větší zisky přináší. Těžební kód tak pracuje na pozadí a nic netušící oběti používají své počítače normálně. Jediným znakem, kterého si mohou všimnout, je pomalejší výkon.

V závěru loňského roku firma Adguard uveřejnila zprávu, že nalezla 33 000 webů, které používají skripty pro dolování kryptoměn. Adguard odhadoval, že tyto stránky měly miliardu kombinovaných měsíčních návštěvníků. Bad Packet Report z letošního února zase hlásí 34 474 webů provozujících Coinhive, což je nejoblíbenější javaScriptový miner, který se ale používá i k legitimnímu dolování.

Nemusíme však chodit daleko. Eset v lednu označil javaScriptový CoinMiner za nejvážnější hrozbu pro tuzemské počítače s podílem až 50 %, což svědčí o mimořádně aktivní kampani. Navíc měl tento malware i podobu trojanů, což nebezpečí této hrozby ještě dále zvyšuje. I když v únoru podíl CoinMineru trochu klesl, stále zůstává nejvýznamnější hrozbou.

Check Point zase zjistil, že škodlivé kódy těžící kryptoměny ovlivnily v prosinci 2017 55 % organizací po celém světě a deset různých variant těchto malwarů se dostalo do Top 100 všech škodlivých kódů, a dvě varianty se dokonce dostaly až do Top 3.

Existují už i specializované botnety jako třeba Smominru, který v lednu 2018 infikoval více než půl milionu Windows serverů, většinou v Rusku, Indii a na Tchaj-wanu. Cryptojacking přitom nevyžaduje významné technické dovednosti – kity jsou k dispozici na darkwebu za pouhých 30 dolarů.

Kryptotěžba je podle analytiků stále ještě v plenkách a existuje mnoho prostoru pro růst a další vývoj. Máme se tedy nač těšit.

Připomínáme, že už za dva měsíce vstoupí v platnost nová směrnice GDPR – buďte na ni připraveni, protože případné pokuty za porušení jsou skutečně obrovské.

A na závěr máme pro vás příjemné překvapení – jako poděkování věnujeme ve spolupráci s firmou Bright Way Solution všem předplatitelům Security Worldu dva licenční kódy pro možnost plně šifrované komunikace přes aplikaci hiddenPrivacy (kódy budou zaslané elektronicky na e-mail). Bližší informace o řešení hiddenPrivacy najdete na stránce 43.

S přáním příjemně stráveného jara i nad stránkami Security Worldu

Pavel Louda
vedoucí projektu

Obsah