MUNI
ICS

Vážený pan
Bc. Kamil Kulíšek
Správa kolejí a menz
Masarykova univerzita
Vinařská 5
602 00 Brno

Váš dopis zn. / ze dne:	Číslo jednací	Vyřizuje / e-mail:	Místo / datum
		Bc. Tomáš Plesník	Brno
		plesnik@ics.muni.cz	19. ledna 2023

Zpráva o výsledcích analýzy těžby kryptoměn na SKM MUNI

Vážený pane řediteli,

dovoluji si Vás tímto informovat o výsledcích analýzy síťového provozu, kterou na Vaši žádost provedl tým CSIRT-MU za účelem odhalení systematické a cílené těžby kryptoměn na zařízeních studentů a hostů SKM MUNI připojených do sítě Eduroam. Tato analýza probíhala dlouhodobě v časových intervalech 4. až 6. října 2022 a následně od 22. října do 21. listopadu 2022. Těžba kryptoměn byla detekována ze zařízení 16 uživatelů v rámci celé sítě Eduroam, ovšem u žádného uživatele se nejednalo o dostatečně trvalou a opakovanou komunikaci (na denní bázi, či po dobu většiny dne), aby vzniklo podezření na cílenou těžbu kryptoměn. Detaily provedené analýzy jsou popsány níže v této zprávě.

V prvním časovém okně se jednalo o manuální analýzu spojení ze sítě Eduroam. Cílem bylo nalézt trvalá spojení na tzv. „mining pools“, jež slouží jako zprostředkovatelé těžby kryptoměn pro koncové uživatele. Agregované síťové záznamy, obsahující množství provozu odpovídající charakteristice těžební komunikace, byly porovnány se seznamem existujících mining pools. Navíc byla zkontrolována i doménová jména spojená s cílovými adresami pro případ, že by prozradily existenci mining pools mimo použitý seznam známých mining pools.

Ve třech dnech komunikace bylo nalezeno hned několik krátkých komunikací s mining pools, nicméně se zpravidla jednalo o krátké časové úseky komunikace, odpovídající například připojení notebooku k Wi-Fi síti v přednáškové místnosti, nebo večerní práci. Žádná z nalezených komunikací tak nejevila známku trvalého charakteru těžby.

Po ověření seznamu těžařských domén byly tyto domény vloženy do detekčního systému týmu CSIRT-MU. V druhém časovém období pak proběhla analýza takto reportovaných událostí. Nejprve byly

extrahovány cílové mining pools a otevřením spojení na tyto adresy bylo ověřeno, zda se nejedná o false positives události. Dále byla analyzována pouze komunikace s mining pools, které odpověděly na dotaz pomocí známého a oblíbeného protokolu pro těžbu kryproměn Stratum [1] [2].

Většina uživatelů, u kterých se komunikace s mining pools potvrdila, komunikovala pouze krátce a nepravidelně, což znamená, že se nejedná o cílenou těžbu kryptoměn. V průběhu času jsme zaznamenali i komunikaci započatou z celkového počtu až 40 zařízení takřka současně, komunikace ale byla velice krátká a nemohla vést k těžbě. S nejvyšší pravděpodobností se tak jednalo o nakažená zařízení uživatelů. Jen pro mobilní systém Android existuje celá řada škodlivých aplikací obsahujících kód pro těžbu kryptoměn bez vědomí uživatele. Je proto velice pravděpodobné, že se budou vyskytovat i v síti MU.

Dle našich zjištění se u žádného z uživatelů nejednalo o dostatečně trvalou a opakovanou komunikaci (denní báze, většina dne), aby vzniklo podezření na cílenou těžbu kryptoměn.

[1] https://braiins.com/stratum-v1

[2] https://braiins.com/stratum-v2

S pozdravem

Bc. Tomáš Plesník
Vedoucí Divize kyberbezpečnosti a správy dat, ÚVT MU
podepsáno elektronicky

Digitally signed by
Tomáš Plesník
19.01.2023