27. 12. 2024

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Phishingový útok na MetaMask peněženku jako (ne)dovolené právní jednání

MetaMask je softwarová peněženka (jednou z nejznámějších a nejpoužívanějších), která funguje jako rozšíření do internetového prohlížeče. MetaMask peněženka uživatelům umožňuje používat kryptoměnu Ethereum a nativní ERC – 20 tokeny, které slouží i jako rozhraní pro v současné době populární NFT tokeny. Kryptopeněženky jsou častým terčem phishingových útoků, zdroje uvádí, že je celosvětově detekováno až 5 milionů těchto útoků ročně. Judikatura je v otázce posuzování takovýchto hackerských útoků velmi strohá. Na jeden případ z nedávné doby se však zaměřím v tomto článku.

Každý uživatel softwarové kryptopeněženky se do ní přihlašuje pomocí vytvořeného **hesla**, což je **Seed fráze spojená s touto peněženkou**, v případě kryptopeněženky MetaMask se jedná o frázi dvanácti slov. Přijde-li uživatel kryptopeněženky MetaMask o Seed frázi (zapomene ji), **ztratí tím navždy přístup ke své kryptopeněžence,** a tedy k obsahu v této peněžence uložené.

Phishing

Phishing (neboli *„rybaření“* či *„rhybaření“*) je podvodná technika spočívající v získávání bezpečnostních hesel, citlivých uživatelských údajů a kódů od uživatelů internetu či sítě mobilních operátorů.[1] V případě kryptoměnových peněženek útočník oběti často podstrčí falešný program či odkaz, které se tváří například jako rozhraní kryptoměnové peněženky.

Právní doktrína uvádí, že tradičně prováděné phishingové útoky, kdy uživatel dobrovolně zadá svá data do „nastrčeného“ programu, je z trestněprávního hlediska nutné posuzovat jako **podvodné jednání** dle ustanovení § 209 zákona č. 40/2009 Sb., trestního zákoníku. Z hlediska soukromoprávního bychom jakožto následek phishingového útoku dle mého názoru uplatňovali nejčastěji **nárok na vydání věci** (vydání odcizeného odkazu MetaMask peněženky), případně **nárok náhradu škody**, pokud by obsah MetaMask peněženky již nebylo dobře možné uvést do předešlého stavu.

Rozsudek Krajského soudu v Praze ze dne 30. 4. 2024, sp. zn. 22 Co 45/2024

V posuzovaném případě se žalobce po žalovaném domáhal **vydání šesti kusů NFT tokenů definovaných na elektronické platformě OpenSea**. Skutkový stav spočíval v tom, že žalobci byly z jeho MetaMask peněženky předmětné NFT tokeny odcizeny phishingovým útokem, kdy se hacker vydával za ředitele a zakladatele jednoho nejmenovaného virtuálního světa, který je v rozsudku anonymizován.

Skutkový stav

Hacker žalobci nabídl **pomoc s jeho problémy při mapování tokenů** v podobě virtuálních pozemků a následně žalobci zaslal phishingový odkaz a vysvětlil mu, že první krok celého procesu mapování tokenů spočívá v tom, že se musí pomocí tohoto odkazu přihlásit do své MetaMask peněženky, a to za účelem zevrubného náhledu a zprovoznění všech jejích funkcí. S využitím autority ředitele a zakladatele anonymizovaného virtuálního světa byl žalobce hackerem donucen propojit peněženku MetaMask prostřednictvím Seed fráze pomocí podvodného odkazu. Následně si hacker stáhl všechny žalobcovy tokeny do své peněženky a začal je prodávat na tržišti OpenSea. Žalovaným ve věci pak byla osoba, která od hackera předmětných 6 NFT tokenů koupila, přičemž se jednalo o žalobu na vydání věci dle ustanovení § 1040 zákona č. 89/2012 Sb., občanského zákoníku.

Svůj nárok žalobce stavěl na ustanovení § 1111 zákona č. 89/2012 Sb., občanského zákoníku, začleněné v pododdílu „**Nabytí práva od neoprávněného**“. Dané ustanovení **vylučuje nabytí vlastnického práva pro věci pozbyté ztrátou nebo činem povahy úmyslného trestného činu**. Předmětné ustanovení zároveň vylučuje vlastnictví pro případy, kdy osoba neprokáže svou dobrou víru v oprávnění převodce převést vlastnické právo k věci.

Rozhodování Krajského soudu

Krajský soud v Praze předně uvedl, že **NFT token je jednotka dat zapsaná do blockchainu, kterou je možné vlastnit a lze s ní obchodovat, je digitálním dílem, movitou věcí nehmotnou** tak, jak upravují ustanovení § 496 odst. 2 a § 498 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, a žaloba je tudíž projednatelná a nárok exekučně vymahatelný.

V meritu věci Krajský soud v Praze potvrdil rozsudek soudu prvního stupně, kterým byla **žaloba zamítnuta**. Své rozhodnutí krajský soud odůvodnil bezprecedentním, lehkomyslným a v digitálním světě **neakceptovatelným a nepochopitelným postupem žalobce, který dle slov soudů obou instancí hackerovi, tedy třetí osobě, poskytl svou Seed frázi v zásadě dobrovolně**. Odvolací soud dodal, že takovéto jednání je jedno z nejhorších provinění vůči vlastnímu majetku, kterého se lze v digitálním světe dopustit.

Odůvodnění

V odůvodnění svého rozsudku dále odvolací soud konstatoval, že **dobrovolné sdělení přístupové Seed fráze k obsahu své MetaMask peněženky nepochybně není možné chránit normami trestního práva**, neboť žalobce nebyl nikým donucen jakékoliv třetí osobě svou Seed frázi sdělit a pokud tak učinil, jednalo se o úmyslné volní jednání **proti pravidlům digitálního světa**, se kterými byl žalobce seznámen prostřednictvím obchodních podmínek MetaMask. Odvolací soud uzavřel, že žalobce svým jednáním fakticky NFT tokeny svěřil třetí osobě a odkázal na ustanovení § 3 odst. 2 písm. c) věty za středníkem zákona č. 89/2012 Sb., občanského zákoníku, dle kterého **nikdo nesmí bezdůvodně těžit z vlastní neschopnosti k újmě druhých**.

Námitka absence dobré víry

S námitkou žalobce o absenci dobré víry žalovaného se Krajský soud v Praze rovněž neztotožnil a v tomto ohledu uzavřel, že u napadeného účtu žalobce na tržišti OpenSea sice v době nákupu předmětných tokenů ze strany žalovaného byla vyznačena poznámka, že *„tento účet je možná napaden*“, nicméně digitální svět má svá specifika, je to svět velmi dravý, dynamický, kde se

jednotlivé kontrakty uzavírají v reálném čase, často v časovém presu, a současně s tím se v digitálním světě předpokládá a je velmi běžná anonymita. Proto dle názoru odvolacího soudu nelze na žalovaného klást vysoké požadavky, co se týče opatřování údajů o historii tokenů či jednotlivých účtů, na kterých byly v minulosti tyto tokeny uloženy. S ohledem na tyto skutečnosti dle názoru odvolacího soudu **žalovaný nepochybně věřil, že tento prodávající uživatel, tj. hacker, řádným vlastnickým titulem k předmětným 6 NFT tokenům disponoval**.

Spear phishing - „harpunové rybaření“

Se závěry soudů obou instancí se neztotožňuji. Právní doktrína rozlišuje formu tzv. **spear phishingu** (neboli *„harpunové rybaření*“). Ta je definována jako sofistikovanější forma phishingu, která je zaměřena na konkrétního uživatele či užší skupinu uživatelů mající určitou společnou charakteristiku. Podvodné zprávy v těchto případech mohou být detailnější, přesnější a cílenější, jejich příprava však zároveň vyžaduje větší úsilí.

Marek Dvořák dále uvádí, že u nejpropracovanějších způsobů realizace spear phishingu je útočník předem v kontaktu s konkrétní osobou více či méně známou vytyčené skupině uživatelů, za niž se následně podvodně vydává, nebo jejímž prostřednictvím následně šíří podvodné zprávy. Pravděpodobnost úspěchu takto provedeného útoku se s ohledem na vyšší důvěru adresátů v odesílatele phishingové zprávy výrazně zvyšuje.[2]

Spear phishing a výše uvedený případ

V nadepsaném případě přitom dle mého názoru útok na žalobce představoval formu výše popsaného spear phishingu. Útočník reagoval na situaci, kdy se žalobce dlouhodobě zajímal o přemísťování pozemků ve virtuálním světě a na skupinové telekomunikační platformě tak dával veřejně najevo. V době útoku byl poměrně čerstvým uživatelem virtuálního světa, když z dokazování vyplynulo, že si MetaMask peněženku založil 4 měsíce před uskutečněním phishingu. **Hacker se navíc vydával za zakladatele a ředitele anonymizovaného virtuálního světa** a s autoritou této osoby žalobci phishingový odkaz pod záminkou zprovoznění všech nezbytných funkcí MetaMask peněženky zaslal.

Trestný čin podvodu dle ustanovení § 209 zákona č. 40/2009 Sb., trestního zákoníku, vyžaduje bezesporu jistou míru obezřetnosti podvedené osoby. Eliška Dostálová přitom rozlišuje 5 hledisek pro stanovení míry nezbytné opatrnosti.[3] Těmi jsou **charakteristika podvedené osoby, sofistikovanost jednání pachatele, ovlivnění jednáním pachatele (důvěryhodnost) a výše majetkové dispozice**. Páté hledisko spočívající ve vědomí poškozeného o (finanční) situaci obviněného nepovažuji pro účely tohoto rozboru za relevantní, neboť nadepsaný případ nemá úvěrový charakter.

Z provedeného dokazování vyplynulo, že Žalobce vstoupil na trh s NFT tokeny jako fyzická osoba v listopadu roku 2021, tedy měl v době předmětného hackerského útoku s metaverzemi zkušenost čítající pouze 4 měsíce. Hacker nezvolil běžnou formu phishingu, ale propracovanější tzv. „spear phishincg“ přizpůsobený na míru žalobci, v reakci na jeho časté dotazy, které na platformě komunity virtuálního světa vznášel. Hacker navíc využil autoritu zakladatele a ředitele tohoto virtuálního světa. Hacker se vyjadřoval gramaticky bezchybně a jeho odborná úroveň se jevila dostatečně vysoká. **Celková hodnota odcizených NFT tokenů z předmětné MetaMask peněženky přitom dle rozsudku činila v nákupní hodnotě částku 1 500 000 USD**.

Závěr

V případě popsaném v tomto článku soudy obou instancí bez dalšího uzavřely, že jednání, kterým žalobce vepsal svou Seed frázi do nastrčeného phishingového odkazu, čímž byl následně obsah jeho MetaMask peněženky vykraden, **představuje v digitálním světě fatální a neomluvitelnou chybu**, kterou žalobce obsah své MetaMask peněženky svěřil neznámé třetí osobě, a kterou **nelze chránit normami trestního práva**, a tudíž nemůže být naplněna podmínka činu povahy úmyslného trestného činu, jak vyžaduje ustanovení § 1111 zákona č. 89/2012 Sb., občanského zákoníku.

Obávám se, že takovýto závěr se může stát nepříznivým precedentem, kdy bude každý phishingový útok v digitálním světě označován za beztrestný. **Dle mého názoru soudy absentovaly na požadavek zkoumání náležité míry obezřetnosti podvedeného, tj. osoby poškozené phishingovým útokem, v rámci trestného činu podvodu**. Pokud by soudy tuto obezřetnost zkoumaly, dospěly by možná k závěru, že se v předmětném případě nejednalo o běžný phishingový útok, v rámci kterého bych žalobcovu neobezřetnost také neomluvila, ale že se jedná o kvalifikovanější formu útoku, tzv. spear phishing, který běžně opatrnému uživateli nedovoluje přiměřeným způsobem rozpoznat, že se o phishingový útok vůbec jedná.

Proti rozsudku odvolacího soudu bylo podáno dovolání, je tedy možné, že zejména posouzení věci po právní stránce, bude změněno.

Mgr. Denisa Mokřížová,
advokátka

Advokátní kancelář Vych & Partners, s.r.o.

Lazarská 11/6
120 00 Praha 2

Tel.: +420 222 517 466
Fax: +420 222 517 478

[1] Boháček, M. Phishing. In: Hendrych, D. a kol. Právnický slovník. 3. vydání. Praha: C. H. Beck, 2009.

[2] DVOŘÁK, Marek. Phishing, pharming a jejich trestněprávní postih. Trestněprávní revue, 2018, č. 4, s. 84-89.

[3] DOSTÁLOVÁ, Eliška. Obezřetnost podvedeného ve světle stávající judikatury. In: Státní zastupitelství, 2022, č. 4.

Další články:

- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti