Kryptoměny v rukou podvodníků

Nákup virtuálních měn se stal velmi oblíbenou a snadno dostupnou činností. Přispěla k tomu nejen vyšší informovanost lidí v dané oblasti, ale i rozšíření sítě tzv. vkladomatů. Různé druhy kryptoměn si tak dnes pořídíte jednoduše např. cestou na nákup nebo prostřednictvím několika kliků v počítači. Existují i uživatelsky zcela jednoduché platební brány pro rychlý nákup kryptoměn platební kartou.
Kde jsou peníze, operují ale i podvodníci. Buďte proto i v souvislosti s kryptoměnami velmi obezřetní.

Zaznamenáváme hned několik typů jednání či souvislostí, při kterých pachatelé trestné činnosti s virtuálními měnami manipulují za účelem svého nezákonného obohacení.

1) Vishing a spoofing

V poslední době hodně diskutované využívání nástrojů sociálního inženýrství, kdy se podvodníci vydávají za bankéře a následně i policisty a pod legendou ohrožení finančních prostředků na bankovním účtu manipulují svoji oběť do provádění finančních transakcí. Nic netušící majitel bankovního účtu z obavy o své peníze převádí peníze přímo podvodníkům.

Ve stejném duchu probíhá také výzva k vybrání hotovosti z „ohroženého“ bankovního účtu a dočasné vložení finančních prostředků do kryptoměn. Tím mají být peníze ochráněny do doby, než se problém s ohroženým účtem vyřeší. Realita je ovšem taková, že tyto peníze nenávratně mizí ve virtuálních peněženkách podvodníků. Vystrašená oběť dostává zcela přesné instrukce i QR kódy, na jaké konkrétní uložiště má za hotovost nakoupenou kryptoměnu odeslat. Oproti online převodům je tento přístup ještě více rizikový. Hotovostní transakce nemůže banka v případě podezření zastavit ani zablokovat, a jakmile je převod na kryptoměnu realizován nejde ho už prakticky nijak zastavit či zvrátit.

Jak nenaletět?

- Vždy si důvody takových telefonátů ověřujte na oficiálních kontaktech bankovních či finančních společností či dalších organizací, za které se podvodníci v dané chvíli vydávají.
- Pamatujte, že banky ani Policie České republiky s provozovateli tzv. vkladomatů nespolupracují.
- Případné ohrožení bankovních účtů klientů řeší banky samy a nepotřebují k tomu zasílání přístupových údajů či údajů z platebních karet.
- Nikdy nenakupujte kryptoměny na adresy, které Vám někdo jiný předá ani je na takové adresy nepřevádějte, pokud nejde o legitimní a vámi zamýšlenou platbu.

Kounicova 24
611 32 Brno

Tel.: +420 974 624 486
Email: krpb.prevence@pcr.cz

2) Falešné investice

Pokud zvažujete, jak zhodnotit své úspory, vybírejte velmi obezřetně, do čeho a s jakými poradci budete investovat. Podvody, ve kterých hrají roli přislíbené vysoké zisky z investic, jsou velmi propracované a naletět je poměrně snadné.

Vše většinou začíná velmi výhodnou nabídkou, např. v podobě internetové reklamy. Vedle investic různého charakteru nabízejí podvodníci také pomoc s nákupem virtuálních měn, často s příslibem velkého výnosu.

Komunikace mezi pachatelem a obětí je většinou dlouhodobá. Oběť je utvrzována, že vše běží podle plánu, např. přístupem do falešného portfolia či virtuálních peněženek na různých demo stránkách. Opět pro zvýšení důvěryhodnosti jsou vyžadovány pravidelné vklady, často s podmínkou vyplacení výnosů až po delším časovém úseku. O tom, že místo zhodnocení finančních prostředků zbydou jen oči pro pláč, se tak poškozený dozvídá až po delší době.

Pachatelé vystupují profesionálně, mají několik úrovní „pracovníků“ (operátory, poradce, techniky, manažery) a jejich legendy jsou propracované s cílem maximalizace zisku.

Pokud chce oběť investované peníze vybrat, přejdou ke strategii komplikací, kdy je nutno zaslat ještě tu „jednu poslední platbu“ a pak už budou velké peníze vyplaceny. Tato psychická manipulace se označuje jako tzv. sunk cost fallacy (česky: utopené náklady). Podstatou je úvaha oběti: „Už jsem do toho dal tolik, teď přece nepřestanu platit, když jsem tak blízko!“

Často oběť podvodníkům, kteří se vydávají za investiční poradce, poskytne kromě osobních údajů, snímků dokladů totožnosti či platebních karet také vzdálený přístup ke svému počítači. K vybílení účtu pak už nebrání prakticky nic.

Jak nenaletět?

- Ke každé investici přistupujte jako k rizikové (obzvláště u kryptoměny) a nikdy k investování či nákupu kryptoměn nepoužívejte celé své jmění.
- Před tím, než se rozhodnete investovat do kryptoměn, zjistěte si, jak fungují velké burzy a investiční platformy a nákup a prodej kryptoměny.
- Vždy pečlivě ověřujte věrohodnost investičního poradce či společnosti. Rozhodně nespoléhejte jen na internetové recenze, ty může napsat kdokoliv, tedy i podvodník.
- Nespoléhejte na to, že podvodný web poznáte podle vzhledu, podvodné stránky investičních platforem bývají profesionálně zpracované, často umožňují vytvoření uživatelského účtu a sledování, samozřejmě podvrženého a fiktivního, portfolia.
- Za žádných okolností neposkytujte vzdálený přístup ke svému počítači.
- Chraňte své osobní, přístupová hesla a údaje z platebních karet.
- Pokud údaje o svém bankovním účtu pod vlivem manipulace poskytnete podvodníkovi, ihned kontaktujte svou banku.
- Pozor na reklamy! Podvodníci si mohou jednoduše zaplatit reklamní kampaň u velké platformy (např. Google, Facebook…) s odkazy na svoje podvodné stránky. Takové reklamy se pak mohou objevit kdekoli, klidně i na prověřených stránkách.

Kounicova 24
611 32 Brno

Tel.: +420 974 624 486
Email: krpb.prevence@pcr.cz

3) Vydíraní přes ransomware

Kryptoměny získávají pachatelé také cestou, při které není nic zastíráno. Šířením ransomware je do zařízení poškozených subjektů instalován škodlivý kód, který šifruje soubory na počítačovém systému nebo omezuje uživatele. Za dešifrování souborů nebo obnovení přístupu je požadováno výkupné, ve většině případů právě v kryptoměnách. V souvislosti s ransomwarovými a malwarovými útoky dochází často i k odcizení dat a výkupné je tak požadováno i za to, že data nebudou prodána či zveřejněna.

Jak nenaletět?

- Chraňte své počítače i mobilní zařízení, zkrátka vše, co připojujete k internetové síti, kvalitním a dostatečným antivirovým programem a firewallem.
- Nestahujte do svých zařízení nic z neověřených zdrojů, neinstalujte podezřelé a neznámé programy, neotvírejte nevyžádané e-maily a jejich přílohy či neověřené odkazy v SMS nebo komunikačních aplikacích (např. Messenger, WhatsApp).
- Zálohujte. V případě napadení zařízení ransomwarem pak můžete svoje důležité dokumenty (účetnictví, rodinné fotografie, pracovní dokumenty) obnovit ze zálohy. Zálohu je potřeba mít oddělenou tak, aby nemohla být také napadena.
- Nástrojem pro šíření malwaru a ransomwaru může být také „pirátsky“ stahovaný obsah, jako seriály, filmy, programy či hry.
- Na stránky se škodlivým obsahem mohou směřovat také reklamy na sociálních sítích a prověřených webech. Pokud vás něco zaujme, neklikejte přímo na nabízený odkaz, ale vyhledejte prezentovaný obsah v některém z vyhledavačů.

por. Mgr. Zdeňka Procházková
oddělení tisku a prevence
Krajské ředitelství policie Jihomoravského kraje