POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

BAKALÁŘSKÁ PRÁCE

2022 OLDŘICH SMETIVÝ

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminalistiky

Aktuální problémy kriminalistické metodiky vyšetřování podvodů

Bakalářská práce

Current problems of forensic methodology of fraud investigation

Bachelor thesis

VEDOUCÍ PRÁCE
Mgr. Jiří Vávra

AUTOR PRÁCE
Oldřich Smetivý

PRAHA
2022

Čestné prohlášení

Čestně prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 10. 03. 2022

Oldřich Smetivý

Poděkování

Na tomto místě bych chtěl upřímně poděkovat panu Mgr. Jiřímu Vávrovi za vedení mé bakalářské práce a především za mimořádnou ochotu a vstřícnost, při poskytování cenných rad. Dále bych rád poděkoval společnosti Surfshark B.V., KvK, za laskavé svolení k užití obrazového materiálu k přípravě této Bakalářské práce.

ANOTACE

Bakalářská práce se zabývá aktuálními problémy během vyšetřování podvodů, ve spojení s moderními nástroji, které užívají pachatelé k páchání trestné činnosti, tak i na celkovém posunu páchání podvodné činnosti do kyberprostoru. Vývoj současných technologií paralelně doprovází dynamický vývoj v páchání trestné činnosti. Práce se dále zabývá prostředky, které má policie proti těmto novým možnostem pachatelů k dispozici.

KLÍČOVÁ SLOVA

Podvod, úvěrový podvod, kyberkriminalita, trestný čin, pachatel, místo činu, důkaz, e-mail, vyšetřování, nástroje pachatelů

ANNOTATION

The bachelor's thesis deals with current issues during fraud investigations, in conjunction with modern tools used by offenders to commit crime, as well as the overall shift in fraud into cyberspace. The development of current technologies is accompanied in parallel by dynamic developments in crime. The work also deals with the means available to the police against these new opportunities for offenders.

KEYWORDS

Fraud, credit fraud, cybercrime, crime, offender, crime scene, evidence, email, investigation, offender tools

Obsah

Úvod

Bakalářská práce se zabývá poznáním aktuálních způsobů páchání podvodů, které užívají pachatelé proti občanům a společnostem na území České republiky. Cílem bakalářské práce je vysvětlit vývoj aktuálního páchání trestné činnosti podvodů a aktuální problémy během vyšetřování podvodů. V této práci jsou rozvedeny nejnovější trendy páchání podvodů, a jejich dosavadní vývoj. Dále jsou v této práci rozvedeny možnosti policie při vyšetřování podvodných jednání a některé nástroje, které pachatelé běžně užívají. Autorem této práce je policista, který je již několik let zařazen do Služby kriminální policie a vyšetřování, na oddělení, jehož úkolem je právě vyšetřování podvodů, zpronevěr, pojišťovací podvodů a kyberkriminality. Autor v této práci rozvedl své několikaleté poznatky vyšetřování podvodů a jaký vývoj během své služby na oddělení vyšetřující podvody vysledoval. Tato práce je sumarizace poznatků zjištěných během vyšetřování podvodů, hlavně přesun podvodného jednání do kyberprostoru. Jsou uvedeny výhody, které to přináší pro pachatele a aktuální problémy jaké to přináší pro Policii České republiky při vyšetřování podvodného jednání.

1 Podvod

Je trestný čin nebo přestupek, jehož pachatel se snaží neoprávněně obohatit na úkor poškozeného. Tato práce se bude zabývat pouze trestnými činy. Pachatel užívá ve svůj prospěch uvedení v omyl, sdělení nepravdy, sdělení pozměněných nebo neúplných údajů a využívá dobré víry a omyly poškozených, ve svůj prospěch. Jako běžné nástroje pachatelů jsou zjišťovány padělané, pozměněné nebo neoprávněně získané písemnosti, osobní doklady nebo jen osobní údaje, případně poskytované informace pachateli poškozeným. Poškozeným může být jak fyzická osoba, tak právnická osoba nebo úřad.

1.1 Obecná charakteristika podvodného jednání

Podvodné jednání se dá obecně charakterizovat jako jednání úmyslné, nečestné, protizákonné, kterým pachatel někoho uvádí v omyl, omyl jiného úmyslně využije s cílem získání osobního prospěchu nebo výhody, případně se neoprávněně obohatit nebo způsobit škodu.

Z obecné charakteristiky lze tedy spatřovat tři znaky podvodného jednání. Prvním znakem je, že osoba podvodně jednající musí jednat úmyslně. Osoba si je vědoma, toho, že jedná podvodně a je to jejím cílem. Druhým znakem je to, že podvodně jednající osoba uvádí jiného v omyl. Velmi často lživým tvrzením, pozměněním údajů, zamlčením informací nebo poskytováním zkreslených informací. Popřípadě podvodně jednající osoba vědoma si toho, že je někdo jiný v omylu tuto situaci využije. Třetím znakem podvodného jednání je to, že osoba podvodně jednajícím nebo využívající omylu jiného jedná v úmyslu obohatit sebe nebo někoho jiného, popřípadě jedná s úmyslem opatřit pro sebe nebo někoho jiného výhodu nebo prospěch, či jedná jen s úmyslem způsobit někomu škodu.

1.2 Právní charakteristika trestného činu podvodu

V České republice je trestný čin Podvod upraven v § 209 odst. 1 zákona č. 40/2009 Sb., v posledním znění a to takto:

„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu

nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“[1]

Subjektivní stránka trestného činu podvodu podle § 209 odst. 1 zákona č. 40/2009 Sb., trestního zákoníku v posledním znění, vyžaduje úmyslné zavinění. Objektivní stránkou uvedeného trestného činu je jednání pachatele v tom, že někoho jiného uvede v omyl, jeho omylu využije nebo zamlčí podstatné skutečnosti, čímž způsobí škodu na cizím majetku. Mezi uvedením v omyl, využitím omylu nebo zamlčením podstatných skutečností, vznikem škody a neoprávněným obohacením pachatele nebo jiného, musí být příčinná souvislost.

Trestní zákoník reflektuje vývoj nových technologií a trendů v technologiích a počítačových systémech a jejich stále většímu nasazení ve firemním a státním prostředí, i jejich integrací do soukromého života fyzických osob. Tím pádem dochází ke stále většímu využívání počítačových technologií pachateli trestných činů. Podle § 110 zákona č. 40/2009 Sb., trestního zákona v posledním znění:

Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.[2]

2 Posun páchání podvodů do kyberprostoru

V posledních letech je patrný přesun pachatelů trestného činu podvodu z „reálného“ světa do kyberprostoru. Aktuálně se jedná o zdaleka nejčastější způsob páchání podvodů a jeho doprovodných trestných činů. Ve statistikách Policie České republiky (PČR) je patrný nárust kyberkriminality od roku 2011, od kdy bylo sledování počtu trestných činů v kyberprostoru zahájeno. V roce 2011 bylo v kyberprostoru zaznamenáno 1502 trestných činů, v roce 2021 jich bylo celkem zaznamenáno již 9518. Na základě statistik PČR celková zaznamenaná

[1] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění.
[2] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění.

kriminalita postupně klesá. Naproti tomu zaznamenaná kyberkriminalita neustále stoupá.[3]

Tabulka 1 Nápad celkové trestné činnosti a kybernetické kriminality, počty zjištěných trestných činů

Rok	Celkový nápad trestné činnosti	Nápad kybernetické kriminality
2011	317177	1502
2012	305428	2195
2013	325366	3105
2014	288660	4348
2015	247628	5023
2016	218162	5344
2017	202303	5654
2018	192405	6815
2019	199221	8417
2020	165525	8071
2021	153233	9518

Zdroj: policie.cz: Kyberkriminalita [online]. [cit. 14. 12. 2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

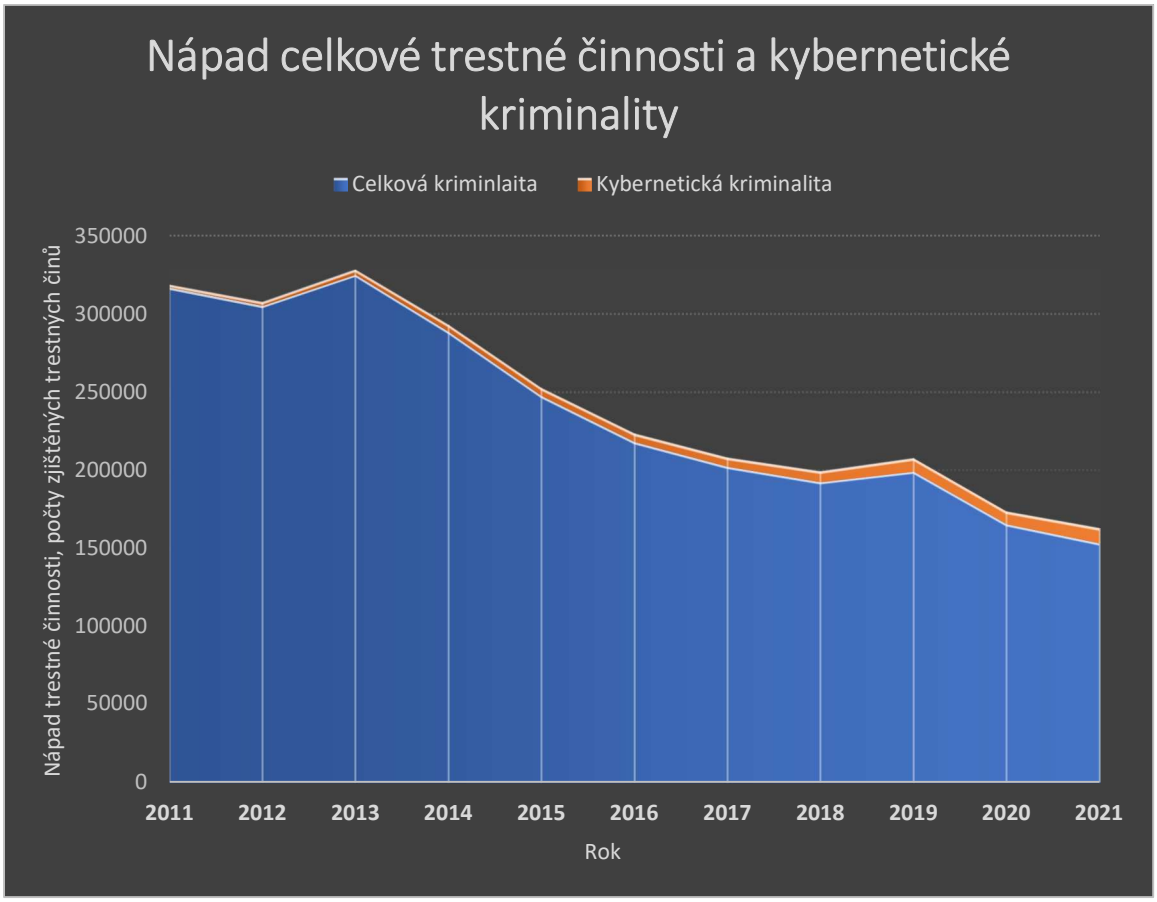
plk. MORAVČÍK Ondřej. Kriminalita klesla o více než 16 procent! [online] 2021. [cit. 14. 12. 2021]. Dostupné z https://www.policie.cz/docDetail.aspx?docid=22588801&docType=ART

plk. MORAVČÍK Ondřej. Vývoj registrované kriminality v roce 2021 [online] 21. 01. 2022. [cit 02. 02. 2022]. Dostupné z https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx

Na následujícím grafu jsou zpracované zjištěné informace. Na vývoji kriminality je patrný sestupný trend. Naproti tomu je zřejmý nárůst kyberkriminality v celkovém počtu evidovaných trestných činů.

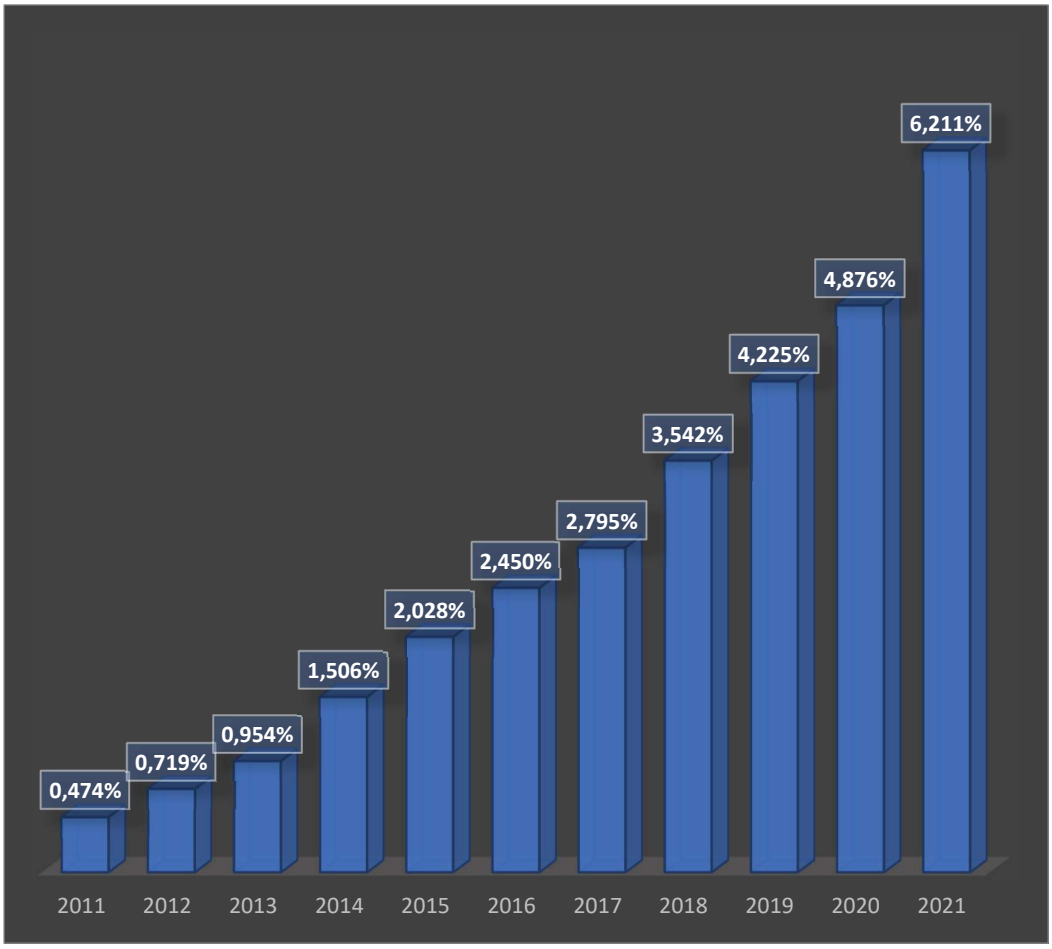
[3] policie.cz: Kyberkriminalita [online]. [cit. 14. 12. 2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.
e-bezpeci.cz: Statistika kybernetické kriminality za rok 2019 [online] 22. 1. 2020. [cit.16. 12. 2021] Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019.
plk. MORAVČÍK Ondřej. Vývoj registrované kriminality v roce 2021 [online] 21. 01. 2022. [cit 02. 02. 2022]. Dostupné z https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx.

Graf 1 Nápad celkové trestné činnosti a kybernetické kriminality



Vzhledem k aktuálnímu vývoji, kdy poměr zjištěné kyberkriminality oproti celkovému nápadu trestné činnosti stoupá, je předpoklad, že bude stoupat i nadále. V roce 2011 tvořil nápad kyberkriminality 0.474 % z celkové zjištěné trestné činnosti. V roce 2021 procentuální část nápadu kyberkriminality stoupla na 6,211 % z celkového nápadu trestné činnosti. Celkový nárůst zjištěné kyberkriminality v počtu zjištěných trestných skutků narostl od roku 2011 do roku 2021 o 534 %. To vše za situace, kdy celkový nápad trestné činnosti od roku 2011 do roku 2021 klesl o 52 %.

Graf 2 Procentuální část kyberkriminality v celkovém nápadu trestných činů



3 Doprovodné trestné činy

Během páchání trestného činu podvodu, v dnešní době zpravidla vídáme další doprovodné trestné činy, které pachatelé páchají v jednočinné i vícečinném souběhu. V těchto případech záleží na aktuálním modu operandi pachatele. Jakým způsobem plánuje provedení svého trestného činu. Cílem pachatele je dopustit se podvodu a ostatní doprovodná trestná činnost poskytuje pachateli potřebné nástroje, další možnosti k navýšení vlastního prospěchu, anebo přístup k informacím, aby mohl pachatel podvod uskutečnit. Pachatel se může dopustit podvodu, ale během toho získá dostatek informací o poškozeném, že se mu podaří sjednat na poškozeného úvěr, čímž se dopustí trestného činu úvěrový podvod podle § 211 z. č. 40/2009 Sb., trestního zákona, v posledním znění

3.1 Právní charakteristika trestného činu Úvěrový podvod

V České republice je trestný čin Úvěrový podvod upraven v § 211 odst. 1 a odst. 2 z. č. 40/2009 Sb., trestního zákoníku, v posledním znění a to takto:

(1) Kdo při sjednávání úvěrové smlouvy nebo při čerpání úvěru uvede nepravdivé nebo hrubě zkreslené údaje nebo podstatné údaje zamlčí, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo bez souhlasu věřitele, v nikoli malém rozsahu, použije prostředky získané účelovým úvěrem na jiný než určený účel.[4]

Subjektivní stránka trestného činu Úvěrového podvodu podle § 211 odst. 1 zákona č. 40/2009 Sb., v posledním znění, vyžaduje úmyslné zavinění, tedy pachatel je si vědom toho, že při sjednávání úvěru uvádí nepravdivé údaje, údaje zkresluje nebo podstatné údaje zamlčí. Objektivní stránkou uvedeného trestného činu je jednání pachatele v tom, že při sjednávání úvěru nebo jeho čerpání poskytne nepravdivé údaje o svém příjmu, kdy pozmění svou výplatní pásku, výpis z bankovního účtu, zamlčí některé své běžné výdaje nebo zamlčí skutečnost, že jeho osoba je již zatížena jiným dluhem apod. V případě spáchání úvěrového podvodu, není ze zákona požadováno způsobení škody věřiteli. Úvěrového podvodu se dopustí i ten, který jedná výše uvedeným způsobem, ale jeho záměrem nebylo někomu způsobit škodu, jeho jednání směřovalo pouze k získání finančních prostředků s tím, že úvěr bude řádně splácet. Není tedy vyžadován úmysl pachatele obohatit se na úkor věřitele. Při vyšetřování trestného činu Úvěrového podvodu je vždy potřeba zvážit okolnosti konkrétní věci. Toto řešil i Ústavní soud České republiky v Nálezu Ústavního soudu ze dne 7. 11. 2006, sp. zn. I. ÚS 631/05.

Má-li v testu proporcionality obstát trestní stíhání úvěrového podvodu, u něhož se v odstavci 1 nevyžaduje vznik škody, pak musí orgány činné v trestním řízení pečlivě zkoumat, zda uvedení nepravdivého údaje bylo v objektivní poloze vůbec způsobilé ohrozit zájem chráněný trestním zákonem, a to jak z hlediska reálného vlivu nepravdivého údaje na úvahu poskytovatele úvěru o návratnosti

[4] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění.

půjčených peněz, tak z hlediska výše reálně hrozící škody, kde je třeba odlišovat podnikatelské a spotřebitelské úvěry. Zdrženlivost je namístě zejména tam, kde měl následný úvěrový vztah standardní průběh, úvěr byl řádně splácen, a kde tedy obavy vyjádřené v hrozbě trestněprávního postihu vůbec nenašly naplnění.[5]

V minulosti byly trestné činy úvěrových podvodů zaznamenávány zejména na menších pobočkách bank a úvěrových společností, kde se pachatelé snažili získat prospěch z poskytnutého úvěru za využití nepravdivých nebo pozměněných informací o své osobě nebo se vydávali za jinou osobu. Tento způsob páchání úvěrového podvodu, až na výjimky zcela vymizel s rozvojem internetových služeb, jako je poskytování úvěrů přes internet, včetně zakládání bankovních účtů přes internet. Uvedený vývoj velmi zjednodušil žádání o úvěrové produkty a bankovní služby, stejně jako tento vývoj zvýšil transparentnost nabízených produktů pro uživatele. Stejnou měrou, ale otevřel nové příležitosti pro páchání trestné činnosti, kdy zejména nebankovní úvěrové společnosti nedostatečně ověřují totožnost žadatele o úvěr a další poskytované údaje od žadatele. Pro spáchání trestného činu úvěrového podvodu, za využití online služeb, nepotřebuje pachatel žádné speciální znalosti počítačových systémů. Pachatelé zpravidla potřebují osobní údaje třetích osob nebo znalost které údaje a jak uvěřitelně pozměnit. Vzhledem k v celku značné nabídce online úvěrů od různých bankovních i nebankovních společností, není problém získat potřebné znalosti formou pokusu a omylu.

3.2 Právní charakteristika trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací

V České republice je trestný čin Neoprávněný přístup k počítačovému systému a nosiči informací upraven v § 230 odst. 1 a odst. 2 zákona č. 40/2009 Sb., v posledním znění a to takto:

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

[5] Nalus.usoud.cz: Vyhledávání rozhodnutí Ústavního soudu České republiky [online] Nález Ústavního soudu ze dne 7. 11. 2006, sp. zn. I. ÚS 631/05 [cit. 28.11.2021]. Dostupné z https://nalus.usoud.cz/Search/GetText.aspx?sz=1-631-05.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

1. *neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*
2. *data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,*
3. *padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná nebo*
4. *neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,*

bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.[6]

V České republice je považováno za trestný čin i neoprávněné získání přístupu k počítačovému systému a nosiči informací i za předpokladu, že na počítačovém systému ani nosiči informací nebude provedena žádná změna, např. výmaz nebo pozměnění dat na daném zařízení uložených, nebude znemožněna nebo omezena funkčnost daných zařízení a informace takto získané (přečtení komunikace, bez pořízení její kopie) nebudou dále nijak zneužity.

3.3 Jednočinný souběh trestných činů

V jednočinném souběhu trestných činů se jedná o situace, kdy pachatel během páchání trestného činu spáchá trestný čin podvod podle § 209 zákona č. 40/2009 Sb., a během tohoto se dopustí dalšího trestného činu. Příkladem trestného činu, který je zpravidla zjištěn v jednočinném souběhu s trestným činem podvodu je Neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 zákona č. 40/2009 Sb., trestního zákoníku v posledním znění. Tento trestný čin je páchán při běžném Podvodu, kdy pachatel přesvědčí poškozeného pod různými

[6] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění.

záminkami, ať už je to pomoc při správě počítače nebo pomoc při různých investicích a operací v internetovém bankovnictví, zpravidla využije neznalost poškozeného a navede poškozeného k instalaci programu pro vzdálenou správu počítače. Většinou se jedná o program AnyDesk nebo TeamViewer. Po té pachatel navede poškozeného k jejich aktivaci. Poškození tak nevědomky zpřístupní pachateli svůj počítač a veškeré údaje v něm uložené. Tímto jednáním tak pachatel naplní skutkovou podstatu trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací, tím, že pachatel získal neoprávněný přístup k počítačovému systému poškozeného, kde pak může podle svých potřeb uložená data v počítačovém systému poškozeného získat, mazat a libovolně měnit. Získané informace pak pachatel zneužije k vlastnímu prospěchu, kterým je zpravidla získán přístup k sociálním sítím, u kterých má poškozený založený účet, bankovním aplikacím poškozeného, stejně jako to, že pachatel disponuje veškerými osobnímu údaji, které měl poškozený uložené v počítačovém systému a je schopen, jménem poškozeného jednat ve veřejné síti internet.

3.4 Výcečinný souběh trestných činů

Příkladem se jedná o situace, kdy pachatel spáchá trestný čin Neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 zákona č. 40/2009 Sb., při kterém se mu podaří získat dostatečné informace o poškozeném. S průběhem následujících dní pak pachatelé zpravidla získaná data užívají pro sovu potřebu, ať už osobní nebo finanční. Získané údaje, zejména kopie osobních dokladů, přístupů na sociální sítě, do internetového bankovnictví a e-mailových schránek jsou dále využívány při páchání další trestné činnosti. Příkladem může sloužit spáchání nebo pokus trestného činu Úvěrový podvod podle § 211 z. č. 40/2009 Sb., při kterém již dříve získané informace a osobní údaje pachatelé užívají k pokusům o získání úvěru, založením online žádosti o poskytnutí úvěru u bankovních nebo nebankovních úvěrových společností. Uvedeným jednáním se může pachateli podařit získat plnění z úvěru, který je ale vedený na poškozeného. Následně velmi často pachatelé pokračují tím, že přepošlou získané finanční prostředky na jiné účty v zahraničí nebo přímo do kryptoměn.

4 Nástroje užívané pachateli

Pachatelé pro konání své trestné činnosti užívají velkou řádku různých nástrojů. Nástroje, užívané k podvodnému jednání, a to zejména v online prostředí vznikají nebo se modifikují již existující prakticky každým dnem. Mezi tyto nástroje započítáváme i prostředky, které pachatelé užívají ke skrytí své činnosti, případně k zamaskování svého podvodného jednání. Dalším velmi častým způsobem užívání nástrojů pachateli je to, že ti to se snaží nebo přímo znemožňují vypátrání své polohy, své totožnosti případně zamaskování nástrojů, které použili přímo k páchání podvodného jednání. Pachatelé pro své jednání využívají velkou škálu nástrojů, ze kterých velká část byla vyvinuta pro legitimní účely a pachatelé pouze zneužívají jejich funkčních schopností k podvodnému jednání a popřípadě k zamaskování své totožnosti a znemožnění jejich vypátrání.

4.1 Legitimní nástroje zneužité k páchání trestných činů

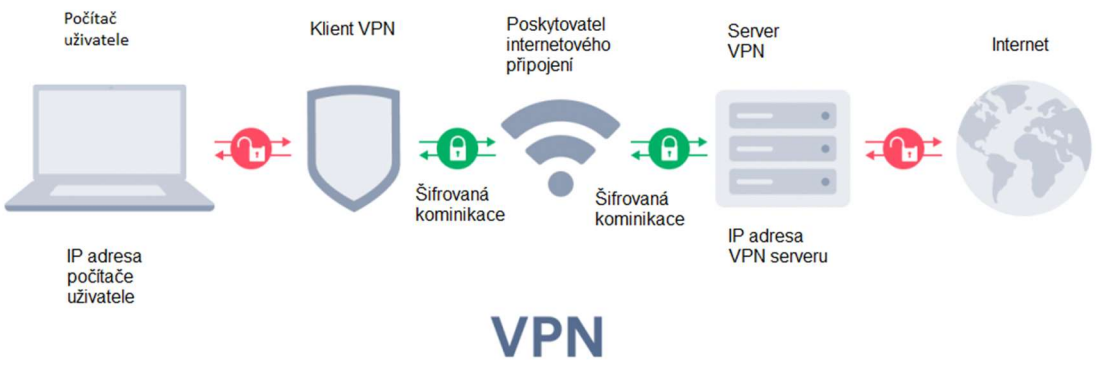
Pachatelé trestných činů si osvojili užívání legitimních počítačových programových nástrojů, které se běžně užívají k jiným činnostem. Příkladem je možné uvést různé free mailové schránky, programy pro vzdálený přístup a chatovací programy. Pachatelé tyto nástroje užívají k páchání trestné činnosti velmi často v originální stavu beze změn softwaru, pouze se jim pomocí sociálního inženýrství a neznalosti běžných uživatelů těchto aplikací nebo neznalostí existence těchto aplikací daří uvádět poškozené v omyl a využívat tak aplikace ve svůj prospěch.

4.1.1 Virtuální privátní síť VPN

Virtuální privátní síť, dále jen VPN, je služba poskytovaná společnostmi soukromým a firemním klientům, která slouží ke zvýšení zabezpečení internetového připojení, zpravidla nezávisle na internetovém připojení. VPN vytváří šifrované internetové připojení od uživatele se servery společností poskytující službu VPN, ze kterých následně probíhá komunikace se zbytkem internetové sítě. Po vytvoření připojení VPN, probíhá od uživatele směrem k serverům poskytovatele služby VPN připojení šifrovaně, čímž zamezuje zjištění obsahu komunikace uživatele všem poskytovatelům internetového připojení, případně odposlechu komunikace (například při připojení k nezabezpečené nebo

již kompromitované Wi-Fi síti). Běžným uživatelům tato služba zvyšuje zabezpečení internetového připojení. Pachatelé tuto službu zpravidla užívají ke znemožnění zjištění své polohy a zabránění zjištění své komunikace internetovým poskytovatelem. Díky užití služeb VPN jsou běžné přístupy pachatelů ke službám nebo napadeným službám poškozených (přístupy na webové schránky, e-mailové klienty, sociální sítě a další), zaznamenány jako přístupy z IP adres serverů poskytovatele VPN, které jsou rozmístěny různě po světě. Čímž pachatelé účinně skrývají sovu IP adresu. Poskytovatelé služeb VPN zpravidla nepořizují žádné záznamy probíhající komunikace nebo historii připojení. Mezi hlavní nevýhody pro pachatele patří to, že se jedná z velké většiny o placené služby.

Obrázek 1 Jak funguje VPN



Zdroj původního obrázku před úpravou: surfshark.com: What is a VPN? Virtual Private Networks 101 [online]. [Cit 30. 12. 2021]. Dostupné z: https://surfshark.com/learn/what-is-vpn.

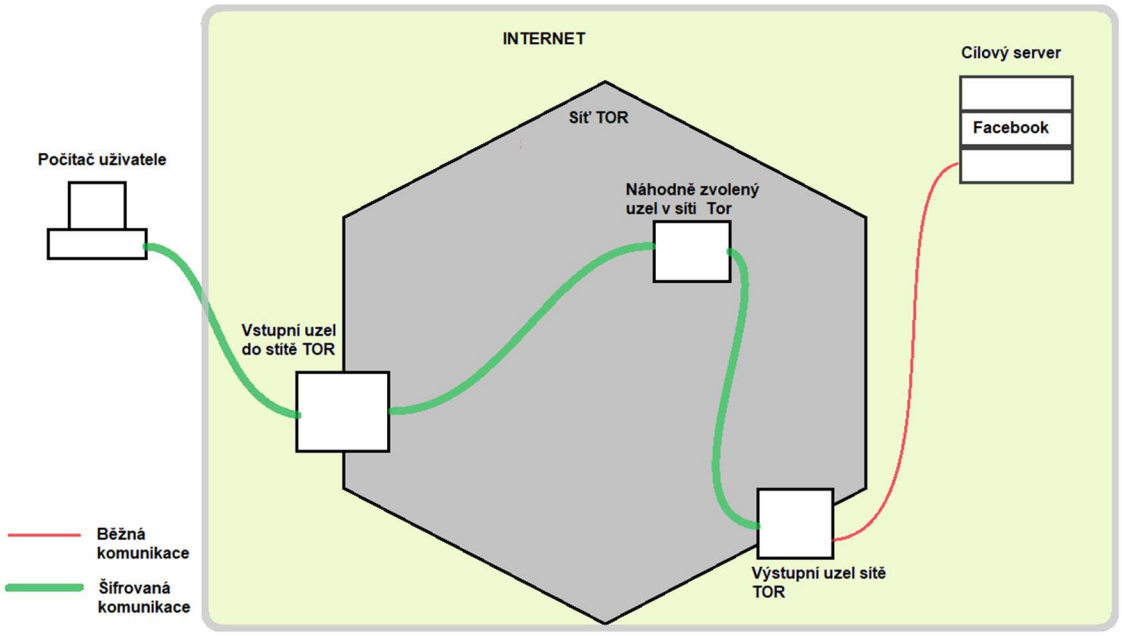
4.1.2 Síť TOR

Síť TOR je nástupcem Onion routing programu, který byl vynalezen ústavem Amerického námořnictva v polovině 90. let. Síť TOR patří k další generaci. Síť TOR je tvořena tzv. uzly, které z velké části vytváří dobrovolníci. Pro přístup k síti TOR je zapotřebí specializovaní internetový prohlížeč. Veškerá komunikace je několikrát šifrována, včetně IP adresy. Připojení po síti TOR je vždy směřováno přes několik náhodně vybraných uzlů, které se mohou nacházet i na různých

kontinentech. Vzhledem k několika vrstvému šifrování je probíhající komunikace skrytá i před správci uzlů. V síti TOR se nachází webové stránky se skrytým umístěním tzv. Onion stránky a další služby. Onion stránky mohou být skryté a hostované v síti TOR. Je možné tyto internetové stránky navštěvovat a užívat bez zjištění serveru, kde se daná Onion stránka nebo služba fakticky nachází. Adresa webové stránky nebo služby v síti tor se skládá z náhodných znaků s koncovkou .onion. Takto vypadá adresa na internetový vyhledavač DuckDuckGo, 3g2upl4pq6kufc4m.onion. Zjištění dat až k cílovému zařízení je prakticky nemožné. Lze zjistit pouze vstupní nebo koncový uzel, nikdy oba najednou. Užití sítě TOR umožňuje procházet internet anonymně, IP adresa uživatele je skryta před webovými stránkami a dalšími internetovými službami. Užitím sítě TOR může pachatel zcela znemožnit zjištění své aktivity na internetu. Mezi hlavní nevýhody této sítě patří vcelku pomalá přenosová rychlost.

Pro přístup do sítě TOR je dále zapotřebí užívat specializovaný webový prohlížeč, který dále vylepšuje anonymitu na internetové síti, tím že o zařízení, na kterém je spuštěn podává k cílové destinaci připojení minimum informací a některé poskytované informace (např. rozlišení displeje přímo podvrhuje). To značně stěžuje a při správném nastavení prohlížeče zcela znemožňuje identifikaci koncového zařízení na základě poskytnutých informací. K tomuto tématu, je třeba zmínit, že TOR prohlížeč už má svou verzi pro mobilní telefony s operačním systémem Android i iOS. Ochrana ve formě TOR sítě a VPN služby se dá kombinovat, tedy lze využít obojí. Na následujícím obrázku, je znázorněn základní princip fungování sítě TOR.

Obrázek 2 Jak funguje síť TOR



4.1.3 Veřejné WI-FI sítě

Veřejné Wi-Fi sítě, se zpravidla nacházejí na místech veřejné přístupných. Veřejné Wi-Fi sítě jsou nejčastěji zřizovány podniky jako benefit klientům. Tyto sítě jsou velmi často zcela nezabezpečené nebo zabezpečené jednoduchým heslem, které je veřejně přístupné. U těchto sítí se zpravidla nezaznamenává, kdo se k nim a s jakým zařízením připojil. Užití veřejně přístupné Wi-Fi sítě může ztížit vypátrání pachatele, protože zjistitelná IP adresa pachatele je zpravidla pouze IP adresa veřejné Wi-Fi sítě. Mezi hlavní nevýhody užití veřejné Wi-Fi sítě patří, že tato je nepřístupná z bydliště pachatele. Pachatel se musí se svým zařízením dostat do pokrytí veřejné Wi-Fi sítě. Pachatel se vystavuje riziku toho, že ho někdo uvidí a zapamatuje si ho. Případně mohou být v okolí rozmístěny kamerové systémy. Riziko stoupá s dobou, po kterou pachatel danou Wi-Fi síť užívá.

4.1.4 Podvodně založené e-mailové schránky

E-mailové schránky neboli elektronické poštovní schránky poskytují elektronické poštovní služby uživatelům. Mezi velmi oblíbené patří tzv. free mailové schránky, které poskytují e-mailové služby zdarma. Free mailové služby poskytují e-mailové schránky na doménách patřící službám, v ČR nejčastěji domény seznam.cz,

centrum.cz, gmail.com a další. Do free mailových schránek se zpravidla přistupuje přes webové rozhraní a protokoly POP3/IMAP[7]. Podvodně založené e-mailové schránky jsou častým a oblíbeným nástrojem pachatelů. Pachatelé užívají rozšířeného modelu free mailových schránek, které nijak neověřují totožnost osoby, která je zakládá. Jedná se o jednoduché a rychlé možnosti změnění základní totožnosti na internetu. K hlavním nevýhodám patří, že free mailové schránky nejsou šifrované, ukládají přístupové údaje a proběhlou komunikaci (pokud není komunikace účelně mazána).

4.1.5 Programy pro vzdálený přístup

Jak už název napovídá programy pro vzdálený přístup jsou užívány pro vzdálený přístup k počítačovému systému, aniž by byla potřeba fyzická přítomnost uživatele u počítačového zařízení. Jedná se o regulérní nástroj užívaný k vzdálenému ovládání počítačových systému, stejně tak jako nástroj hodně užívaný softwarovou a počítačovou podporou, případně firemními správci, která umožňuje zásah do počítačového systému bez příjezdu technika. V domácích podmínkách se tyto programy používají pro vzdálené ovládání domácího počítače, třeba prostřednictvím mobilního telefonu z terénu a umožňují tak přístup k souborům a informacím v počítači uloženým. Mezi oblíbené programy patří aplikace TeamViewer a AnyDesk. V současnosti pachatelé využívají tyto programy, kdy se po telefonickém rozhovoru vydávají za obchodníka banky, anebo softwarovou podporu Microsoft, a navedou počítačově nezdatného uživatele k instalaci jednoho z uvedených programů nebo jejich obdobě. Při telefonickém rozhovoru provedou poškozeného krok za krokem k aktivaci, kdy pak mimoděk poškozený zpřístupní pachatelům celý svůj operační systém a data v něm uložená. Velmi často se podaří pachatelům díky tomuto systému a výborným komunikačním dovednostem překonat i dvou faktorové zabezpečení internetového bankovnictví poškozených a získat tak plný přístup k internetovému bankovnictví poškozeného. Díky čemuž se jim podaří získat veškeré finanční prostředky na bankovních účtech poškozeného a v některých případech se pachatelům podaří i zažádat o úvěr

[7] POP3 – Post Office Protokol v.3 (poštovní protokol verze 3), užitím tohoto protokolu, stahuje e-mailový klient zprávy ze serveru do zařízení.
IMAP – Internet Message Access Protokol (Protokol pro přístup ke zprávám v internetu), užitím tohoto protokolu manipuluje e-mailový klient se zprávami přímo na serveru.

jménem poškozeného. Není výjimkou, že poškozený sleduje celé dění na svém monitoru.

4.1.6 Neregistrované SIM karty

Neregistrované SIM karty neboli SIM karty na kredit s předplacenými jednotkami jsou jedním ze základních a nejjednodušších prostředků které pachatelé využívají k zakrývání své vlastní totožnosti. Jedná se o velmi levnou a jednoduchou možnost, jak zakrýt svou totožnost. Výhodou pro pachatele je, že těchto SIM karet je na trhu nespočet a pachatelé tak mohou velmi často měnit své telefonní číslo. Nevýhodou pro pachatele je, že operátoři zaznamenávají nejen číslo SIM karty a telefonní číslo, ale také IMEI zařízení, které se do sítě připojilo, proto se jedná pouze o základní možnost zakrytí své pravé totožnosti. Orgány činné v trestním řízení mají přístup k číslu IMEI (International Mobile Equipment Identity – Mezinárodní identita mobilního zařízení) a k poloze daného zařízení v čase, tedy odkud a na jakou síť, k jaké buňce a kdy se jaké zařízení připojovalo.

4.1.7 Kryptoměny

Kryptoměny jsou elektronické peníze, u kterých se však nejedná o oficiální měnu státu, kterou spravuje centrální banka.

Kryptoměny finanční správa považuje z pohledu českého soukromého práva za věc v právním smyslu, a to za věc nehmotnou, movitou a zastupitelnou. Z dostupných stanovisek ČNB vyplývá, že Bitcoiny nejsou bezhotovostní peněžní prostředky ani elektronické peníze, nákup nebo prodej Bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb ani bezhotovostní obchod s cizí měnou podle zákona o platebním styku (č. 284/2009 Sb.). Směna Bitcoinů za oficiální měnu nenaplňuje znaky směnárenského obchodu a Bitcoiny nevykazují ani znaky investičního nástroje – nemají povahu ani cenného papíru ani derivátu.[8].

Vždy se jedná o decentralizovaný systém, který nemá centrální autoritu, měnu nekontroluje žádná centrální banka ani instituce nebo vláda. Transakce kryptoměn probíhají na přímo mezi obchodujícími bez prostředníků. Kryptoměny se vyznačují

[8] HOVORKA Jiří. Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc [online] 2017 [cit. 03. 01. 2022]. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/.

silným šifrováním a s transakcemi nejsou spojeny žádné osobní a citlivé údaje, pouze označení peněženky, ze které a do které transakce probíhá. V případě kryptoměny Bitcoin jsou veškeré transakce uložené v centrální databázi takzvaném Blockchainu, jehož kopie jsou rozmístěné různě po světě. Každá transakce je vždy zaznamenána v blockchainu, a tedy zpětně dohledatelná. Jsou ovšem kryptoměny, které jsou zcela anonymní a transakce jsou nedohledatelné. Jako příklad může sloužit kryptoměna Monero.

4.1.8 Chatovací aplikace

Velmi rozšířenými nástroji pachatelů, které používají k páchání trestné činnosti, a hlavně k prvotnímu kontaktu s poškozeným, jsou mobilní chatovací aplikace jmenovitě WhatsApp iMessage a Messenger. Pachatelé velmi často využívají jednoduchost přihlášení se k službám těchto chatovacích aplikací. Jmenovitě lze uvést aplikaci WhatsApp, u které stačí vlastnit pouze telefonní číslo nebo SIM kartu s telefonním číslem pro prvotní instalaci aplikace a její zprovoznění. Následně může aplikace fungovat samostatně na internetové síti nebo pomocí klienta na počítači. Pachatelé také zneužívají funkci šifrování komunikace mezi různými klienty, kdy využívají toho, že běžný internetový provoz tuto komunikaci nezachytí a nejde dešifrovat. Pokud je potřeba pro potřeby trestního řízení zajistit komunikaci, příkladem z aplikace WhatsApp. Je zapotřebí znalcem zajistit komunikaci z telefonního přístroje, kde tato komunikace probíhala tedy z telefonního přístroje pachatele. Toho se dá použít pouze za předpokladu, že pachatel pravidelně svou komunikaci nepromazává a PČR během vyšetřování získá přístup k uvedenému mobilnímu telefonu.

4.2 Nástroje přímo vyvinuté k páchání trestných činů

Pachatelé pro páchání trestných činů vyvíjejí i specializované nástroje. V těchto případech se již jedná o specializované osoby v oblasti IT. Není výjimkou, že specializovaní hackeři vyvíjejí specializované nástroje pouze za účelem prodeje, aniž by měli v úmyslu je někdy použít. Existují celé obchodní a prodejní sítě na hackerské nástroje umístěné na Dark Webu[9]. K nákupu a prodeji nástrojů dochází

[9] Dark web je součástí Deep Webu. Obsah Dark Webu není dohledatelný běžnými vyhledávači není indexován. Dark Web užívá také síť TOR

na Dark Web a platby probíhají formou kryptoměn. Na Dark Web je možnost objednat i služby hackerů k přímému útoku na jedince, společnost nebo instituci.

4.2.1 Phishing

Jedná se z největší části o podvodné e-mailové zprávy, které se vydávají za legitimní zprávy zaslané od důvěryhodných institucí jako jsou banky, pošta apod. Účelem těchto Phishingových je zpráv získání citlivých údajů poškozených nebo rovnou přístup do internetového bankovnictví. Zpráva povětšinou obsahuje odkaz na podvržené stránky dané instituce, za kterou se Phishingová zpráva vydává. Tyto stránky se tváří jako zcela legitimní, ale jsou pod plnou kontrolou pachatele. Zpravidla přihlašovací stránka určité banky do internetového bankovnictví. Tímto způsobem se daří pachatelům obejít i dvou faktorové zabezpečení, kdy poškozený sdělí pachatelům prostřednictvím podvržených stránek i zaslaný bezpečnostní kód.

4.2.2 Vishing

Vishing je obdoba Phisingu, ale páchaná cestou telefonních hovorů. V případě Vishingu, který se v posledním roce velmi rozšířil, pachatel za užití internetových služeb podvrhne telefonní číslo banky a telefonuje klientům banky, kde se pod zobrazeným (na telefonu poškozeného) pravým číslem bankovní instituce představí jako bankéř. Po krátkém rozhovoru pachatel navodí u poškozeného dojem ohrožení jeho bankovních účtů a přesvědčí poškozeného k převodu finančních prostředků do kryptoměn nebo za užití aplikace pro vzdálený přístup převezme kontrolu nad bankovním účtem poškozeného skrz počítač poškozeného. Byly zachyceny případy, kdy se pachatelé vydávali i za policisty a telefonovali z podvržených policejních telefonních čísel. Dalším velmi častým způsobem Vishingového útoku, který je celosvětově rozšířený i díky rozšířenému anglickému jazyku, je způsob, kdy se pachatel vydává za podporu společnosti Microsoft. V tomto případě pachatel přesvědčuje poškozeného o napadení jeho počítače virem a velmi často vyhrožuje odpojením daného systému od internetové sítě. Pachatel u poškozeného navodí dojem, že jeho počítačový systém je nakažený virem a zapůsobí na svědomí poškozeného, kdy poškozenému vysvětluje, že jeho počítač je dále užíván k šíření virů a napadání dalších počítačů.

Poté zpravidla pachatel navede poškozeného ke stažení aplikace pro vzdálený přístup k počítači, kterou mu pomůže po telefonu nastavit. Následně pachatel získá přístup k počítači poškozeného a ke všem datum v něm uloženým, velmi často včetně přístupu do internetového bankovnictví.

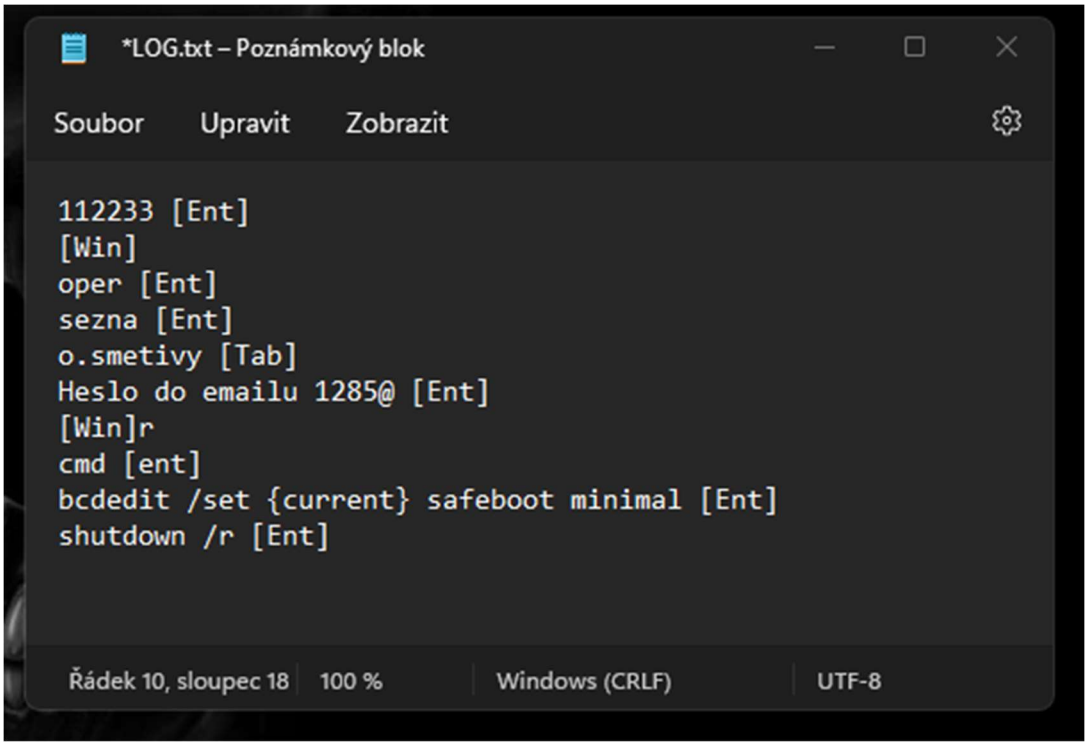
4.2.3 Keylogger

Keylogger je program, který zaznamenává veškeré stisky kláves na počítači a ukládá je. Periodicky pak odesílá záznam kláves pachateli, který tak získá kompletní záznam přihlašovacích údajů a všeho co poškozený napsal na klávesnici. Keylogger je škodlivý program, který je zpravidla skrytě naistalován hluboko v systému počítače. K infekci počítače nejčastěji dochází při stažení nakaženého souboru z neověřeného zdroje nebo bývá součástí nakaženého instalačního souboru. Keyloggery jsou na trhu dostupné také jako hardwarové komponenty. Jsou ve formátu průchozího USB zařízení, a zapojují se mezi kabel klávesnice a počítačovou skříň. Výhodou tohoto zapojení je jeho nemožnost detekce systémem a je schopen zaznamenávat stisknuté klávesy již před zavedením systému. Nevýhodou, je že útočník musí mít fyzický přístup k počítači.

Na notebook autora byl naistalován Keylogger[10]. Poté byl notebook restartován a autor se přihlásil do systému, otevřel internetový prohlížeč Opera a přihlásil se do free mailové schránky na adrese seznam.cz. Následně byl otevřen příkaz spustit, byl otevřen příkazový řádek. V příkazovém řádku byly zadány příkazy pro příští restart systému do nouzového režimu a konečně byl zadán příkaz k restartu systému. V logu Keyloggeru je patrné, že pin pro přihlášení do systému je 112233, autor vlastní e-mailovou schránku na adrese seznam.cz a jeho přihlašovací údaje jsou jméno: „o.smetivy“ a heslo „Heslo do emailu 1285@“. Na tomto příkladu je patrné, že ani vcelku bezpečné heslo (v tomto případě 21 znaků, velká a malá písmena, číslice a speciální znaky) není dostatečným zabezpečením, pokud jsou takovéto údaje použity na nezabezpečeném počítači. Níže je pořízený výstřižek logu, který zaznamenal Keylogger, ve kterém jsou zaznamenány veškeré, klávesy, které autor použil k výše uvedeným úkonům.

[10] Keylogger dostupný na https://github.com/GiacomoLaw/Keylogger. MIT License, Copyright (c) 2017 Giacomo Lawrance

Obrázek 3 Záznam Keyloggeru



4.2.4 Ransomware

Ransomware je škodlivý program, který zašifruje data uložená na pevném disku počítače a dalších discích nebo přepisovatelných paměťových mediích, a tak znemožní přístup uživatelům k jejich souborům nebo zcela znemožní funkci počítače. Ransomware následně po zašifrování dat zobrazí vyděračskou časově omezenou výzvu k zaplacení výkupného, často formou Bitcoinu na Bitcoinovou peněženku pod kontrolou pachatelů. Poškozený za platbu výkupného následně obdrží dešifrovací klíč. K infikaci Ransomwarem zpravidla dochází z infikovaného souboru staženého z internetu nebo z přílohy e-mailové zprávy, případně návštěvou infikované internetové stránky. Napadený počítač je pak z velké většiny schopen infikovat další počítače připojené k místní síti. Díky této vlastnosti byly zaznamenány případy, kdy byly zašifrovány veškeré počítače v místí síti nemocnic, institucí a firem, a tak znemožnili jejich fungování a zničil jejich veškerá počítačová data. Vysoká „infekčnost“ Ransomwarových virů způsobila i zničení veškerých nízce zabezpečených záložních datových systémů.

4.2.5 Adware

Adware je bezplatný program, který vydělává svým vývojářům zobrazením reklamy a vyskakovacích oken uživateli počítače. Jedná se o aplikace, které slibují poškozeným funkce zdarma. Většina Adware programů je pouze obtěžujících, byly ale zachyceny i programy, které zaznamenávaly osobní informace uživatelů nebo obsahovaly Keylogger.

4.2.6 Počítačový virus

Počítačový virus je program nebo část kódu, který se na počítačovém systému spouští skrytě, bez vědomí uživatele. Jeho účelem je ovládnutí počítačového systému nebo destruktivní akce na infikovaném systému. Počítačový virus pak zpravidla používá nakažený počítač ke své vlastní replikaci a infikaci dalších počítačových systémů. Počítačové viry se zpravidla skrývají do programů, doplňků prohlížečů, instalačních souborů z neověřených zdrojů.

4.2.7 Trojský kůň

Trojský kůň je povětšinou program, který se tváří jako legitimní program, který uživateli přináší nějaké funkce navíc, v některých případech se trojský kůň tváři i jako antivirový program. Výhodou trojského koně z pohledu pachatele, je to, že si jej uživatel zpravidla naistaluje do počítačového systému dobrovolně. Trojský kůň pak na infikovaném počítačovém systému způsobuje destrukci dat nebo krádeže dat.

4.2.8 Sociální inženýrství

Sociální inženýrství není nástroj jako takový, je to soubor znalostí. V kontextu podvodů, se o Sociálním inženýrství nemluví z hlediska společenské vědy, ale jedná se o nástroj manipulace poškozených pro dosažení určitého záměru. Jedná se o soubor znalostí chování lidí a jak je využít. V současné době se jedná o nejsilnější nástroj pachatelů při páchání trestných činů. Tak jak se s časem zlepšuje zabezpečení bankovních systémů a dalších internetových aplikací, bývá nejslabším článkem zabezpečení právě uživatel. Pachatelé dávno zjistili, že překonat zabezpečení „brutálním“ útokem na infrastrukturu, anebo virovou infekcí v počítači je mnohem složitější než prostě poškozeného přesvědčit o tom, aby se

sám nevědomky vzdal přístupu ke svému internetovému bankovnictví nebo ho uvést v omyl tak, že pachatelům v podstatě odevzdá veškeré své finanční prostředky. Díky správně navrženému Phishingovému nebo Vyshingovému útoku za, správného využití informací získaných sociálním inženýrstvím se nemusí pachatel zabývat ani tím, jak je internetová aplikace nebo internetové bankovnictví zabezpečeno, protože poškozený pachatele do internetového bankovnictví nebo počítačového systému vpustí sám a dobrovolně. Jedná se o znalosti získané léty spamových e mailových kampaní a jejich jednoduchou analýzou, na které způsoby, spamové reklamy nebo spamové podvody lidé nejčastěji reagují. Pokud jde o sociální inženýrství v dnešní době nejčastěji užívané, toto se dělí na základní principy lidského chování. Sociální inženýrství využívá různé vlastnosti psychiky poškozených zejména strach, závist, chamtivost a zvědavost na jedné straně a druhé straně využívá neznalost poškozených v počítačových systémech, neochotu se o tyto systémy zajímat a zdokonalovat se v jejich ovládání a fungování a dále také lenost poškozených vyhledávat ověřené informace z ověřených zdrojů na internetu. Sociální inženýrství je velmi úspěšně využíváno u různých Phishingových a Vyshingových podvodných kampaní, stejně tak jakou spamových kampaní. V poslední době je jako nejčastější Modus operandi se ve Vyshingovém podvodu objevuje způsob, kdy se pachatel vydává za bankéře banky poškozeného. Následně poškozeného přesvědčí, že jeho celoživotní úspory jsou v nebezpečí a díky velmi dobré komunikační schopnosti a znalosti sociálního inženýrství poškozeného přesvědčí o převodu svých finančních prostředků do kryptoměn nebo využije neznalosti poškozeného v počítačových systémech a získá přístup přímo do internetového bankovnictví poškozeného. Podobným způsobem jsou koncipovány Phishingové e-mailové zprávy, které pachatelé rozesílají poškozeným. Většina těchto Phishingových e-mailových zpráv má navodit u poškozeného dojem, že jeho životní úspory nebo bankovní účet je v ohrožení nebo že došlo k prolomení jeho zabezpečení a poškozený je pak následně vyzván k tomu, aby své přihlašovací údaje včetně ověřovacích kódů zadal na podvodnou internetovou stránku. Tyto e-mailové zprávy se s časem velmi zlepšují, kdy v dnešní době už není jednoduché rozpoznat podvodnou e-mailovou zprávu od oficiální komunikace s bankou. Pachatelé velmi dobře napodobují správný formát e-mailu banky včetně veškeré grafiky a stylizace.

5 Běžné typy podvodů zachycené na území ČR

Dlouhodobým sledováním trendů páchání podvodů bylo možno vysledovat několik základních typů způsobů páchání. Není ovšem výjimkou kombinace několika způsobu páchání jedním pachatelem na jednoho poškozeného. Různé trendy v páchání podvodů na internetu se objevují ve vlnách, často v rámci reakce na aktuální dění ve světě nebo na sociálních sítích.

5.1 Falešný bankéř

Jedním z nejmodernějších způsobů páchaní podvodů. Jedná se o v poslední době velmi rychle stoupající trend v páchání. Podvod začíná zpravidla tím, že je poškozený kontaktován telefonicky osobou, která se vydává za zaměstnance banky, u které má poškozený vedený bankovní účet. Vyšetřováním aktuálně prověřovaných trestných činů vyplývá, že osoba, která telefonuje poškozenému je již dopředu velmi dobře informována o poškozeném. Není výjimkou, že podvodný bankéř zná o poškozeném jeho základní osobní údaje jako je jméno, e-mailová adresa, adresa fyzického bydliště a konkrétní banku u které má poškozený vedený svůj bankovní účet. Falešný bankéř pak velmi často v poškozeném vzbudí dojem, že jeho finance jsou v nebezpečí nebo že na jeho osobu byl proveden pokus o získání úvěru a po celou dobu vystupuje v pozici pomocníka poškozenému. Následně pak falešný bankéř přesvědčí poškozeného, aby mu pod záminkou pomoci zpřístupnil svůj počítač užitím programu pro vzdálenou zprávu počítače, čímž získá přístup do internetového bankovnictví. Další variantou je, že falešný bankéř přesvědčí poškozeného o úplném výběru jeho finančních prostředků a jejich vložení do Bitcoinmatu, buď přímo na peněženku falešného bankéře nebo na bitcoinovou peněženku poškozeného, kterou ale zakládal za pomoci falešného bankéře a ten k ní má také přístup. Tento způsob páchání podvodné činnosti je pro poškozené velmi nebezpečný, protože poškození velmi často přijdou o všechny své úspory a v některých případech skončí i zadlužení, protože falešný bankéř si na poškozené založí úvěr. Z doposud zjištěných informací vyplývá, že banky takto odcizené peníze neproplácí zpět, s tím odůvodněním, že poškození porušili smluvní podmínky, které podepsali při zakládání účtu a předali své přístupové údaje nebo umožnili přístup do svého bankovnictví 3. osobě.

5.2 Nigerijské podvodné dopisy

Jedná se o klasický podvod, který zpravidla začíná nevyžádaným e-mailem, ve kterém je příjemce zprávy žádán o pomoc při převodu velké finanční částky z Afriky. Odesílatel se představuje jako majitel diamantového dolu, člen prezidentské rodiny, potomek krále, voják apod. Jako odměna pro poškozeného je často uváděna možnost značného výdělku za pomoc při převodu finančních prostředků. Napřed je, ale po poškozeném vyžadováno zaplacení spousty nesmyslných poplatků za převod, za založení účtu a dalších smyšlených správních poplatků. Není výjimkou, že poškození zašlou pachateli kompletní kopie svých osobních dokladů.

5.3 Výherce loterie

Jedná se o adaptaci Nigerijského podvodu. Tyto série se vyskytují zpravidla poté, co je nejčastěji na území USA zveřejněna totožnost výherce v loterii. V tomto případě je většinou úvodní e-mail vysvětlený legendou, že výherce neví, co má s tolika penězi dělat, tak se rozhodl pomáhat různě po světě a o svou výhru se dělí. Věrohodnost těchto e-mailu je zdánlivě podporována užíváním jména výherce (pokud bylo zveřejněno). Následuje ovšem zaplacení spousty nesmyslných poplatků za převod, za založení účtu a dalších smyšlených správních poplatků. Není výjimkou, že poškození v období několika měsíců odešlou na smyšlené poplatky na účty různé po světě i částky převyšující milion korun.

5.4 Indický podvod

Jedním z velmi rozšířených podvodů, hlavně v anglicky mluvících zemích je Indický podvod. V těchto případech pachatel volá poškozeným a předstírá, že pracuje na lince podpory společnosti Microsoft. Následně pachatel pod různými záminkami, jako je poškození operačního systému počítače poškozeného nebo jeho domnělá infekce počítačovými viry, získá za pomoci programů pro vzdálený přístup vládu nad počítačem poškozeného. Následuje pak proniknutí do internetového bankovnictví poškozeného nebo zcizení přihlašovacích údajů k dalším službám.

5.5 Falešné inzeráty

Dalším běžným způsobem páchání podvodů na internetu jsou falešné inzeráty. Tyto se dělí do dvou základních kategorií. A to na podvodné inzeráty na bazarových webových portálech a na podvodné inzeráty na sociálních sítích, nejčastěji Facebook.

5.5.1 Podvodné inzeráty na bazarových webových portálech

Jedním z nejjednodušších podvodů páchaných na internetu jsou podvodné inzeráty na webových bazarových portálech. Na území České republiky se nejčastěji jedná o podvodné inzeráty na webových portálech bazos.cz a sbazar.cz. V těchto případech je nabízené levné zboží, za které pachatelé požadují platbu předem, anebo značnou zálohu. Objednané zboží, ale ve většině případů není ani majetkem pachatele a ten jenom zneužívá fotografie produktů, které nalezl na internetu. Jedná se o velmi rozšířený typ podvodu. Spousta pachatelů takovéto trestné činnosti nabízí levné zboží a spoléhá na to, že vzhledem k malým škodám nedojde ve velké většině ani k nahlášení skutku na policii. V poslední době se začíná objevovat sofistikovanější varianta uvedeného podvodu. V této variantě si pachatelé vytvoří falešnou webovou stránku, u které často zneužívají dobré jméno inzertních serverů, na kterém zveřejnili své podvodné inzeráty. Podvodné stránky pak svádí poškozené k vyplnění svých platebních údajů, pod záminkou zabezpečení platby, s tím, že toto spravuje webový bazarový portál. Tyto podvodné stránky jsou, ale pod kontrolou pachatele.

5.5.2 Podvodné inzeráty na sociálních sítích

V tomto případě se jedná o rozšíření podvodných inzerátů na sociálních sítích, nejčastěji s nabídkou různých investic. V poslední době nejčastěji do kryptoměn. Tyto podvody mají často zahraničního pachatele, který je schopen vytvořit věrohodnou legendu investiční společnosti, včetně dobře propracovaných webových stránek s možností přihlášení uživatele a vytváření uživatelských účtů. Takovéto podvržené stránky smyšlené investiční společnosti, často fungují na principu podvržení poskytovaných údajů poškozeným. Poškozený zpravidla po přihlášení ke svému účtu na těchto internetových stránkách vidí svůj domnělý zisk

a nárůst hodnoty jeho investice. To, že se jedná o podvod většinou poškozený zjistí až v momentu, kdy chce vybrat zisk z investice nebo stáhnout celou investici. V takovýchto případech je poškozený vystaven nekonečným obstrukcím ze strany údajné investiční společnosti a není výjimkou, že poškozených dále zaplatí řadu nesmyslných poplatků, ve snaze získat své finanční prostředky. Tímto svým jednáním se pachatelé snaží prodloužit fungování svých podvržených investičních portálů, aby co nejvíce oddálili situaci, že poškození nahlásí podvod na policii, anebo na webových fórech vyjde najevo, že investiční portál je pouze podvod

5.6 CEO podvody

Mezi vzácnější podvody patří CEO podvody (chief executive officer – Výkonný ředitel). Jedná se o typ podvodu, ve kterém v rámci komunikace (nejčastěji e-mailové komunikace) uvnitř společnosti nebo v rámci komunikace mezi dvěma společnostmi se podaří do komunikace vniknout 3. osobě. Tato 3. osoba (pachatel) poté na obě strany posílá věrohodné e-mailové zprávy nebo zadržuje a pozměňuje e-mailové zprávy a využívá omylů pracovníků společnosti, kteří pak pod legitimními záminkami zasílají platby za zboží nebo za poskytnuté služby na podvržené bankovní účty. Pachatelé velmi často využívají situace, kdy obě společnosti se nenacházejí ve stejné zemi a při odesílání faktury z jedné společnosti na druhou tuto fakturu pozmění a doplní zde číslo svého bankovního účtu nebo sami odešlou e-mail se zprávou, že z finančních nebo politických důvodů došlo u společnosti, která vystavila fakturu ke změně bankovního účtu a žádá poslat platbu na nový bankovní účet, zpravidla v jiné zemi. U těchto podvodů policie registruje škody i v milionech korun za jednu podvrženou fakturu. Vzhledem k tomu že mezinárodní komunikace mezi společnostmi často probíhá v anglickém jazyce, není problém pro pachatele věrohodně pozměnit nebo podvrhnout e-mailovou zprávu. Další variantou tohoto podvodu jsou potvrzené e-mailové zprávy v rámci jedné společnosti. V tomto případě se pachatel v e-mailové komunikaci vydává za vedoucího pracovníka. Poté v e-mailové komunikaci smyšlený vedoucí pracovník zpravidla zasílá příkazy k platbám nebo smyšlené faktury účetním společnosti s pokyny k platbě za tyto faktury, na účet pod kontrolou pachatele.

6 Prostředky PČR

PČR užívá k vyšetřování případů nástroje podle zákona č. 141/1961 Sb., o trestním řízení soudním a zákona č. 273/2008 Sb., o Policii České republiky. Dále spolupracuje se soukromými subjekty, zejména při získávání záznamů internetové komunikace a komunikace prostřednictvím mobilních sítí. Ve spolupráci PCŘ se soukromými subjekty zjišťuje údaje o uživateli různých internetových služeb. Velmi často PČR při vyšetřování spolupracuje s orgány činnými v trestním řízení v jiných zemích, a to v zemích Evropské unie i mimo ni.

6.1 Podpůrné operativně pátrací prostředky

Podpůrné operativně pátrací prostředky užívá PČR již před zahájením trestního stíhání, při získávání poznatků o trestné činnosti. Účelem podpůrných operativně pátracích prostředků je hlavně získávání poznatků páchané trestné činnosti a získávání poznatků pro potřeby trestního řízení. Užívání podpůrně pátracích prostředků policistou se řídí zákonem o Policii České republiky a jsou upraveny v §72, §73, §74, §75, §76 a §77 z. č. 273/2008 Sb., o Policii České republiky, v posledním znění.

Policista je při předcházení trestným činům, při získávání poznatků o trestné činnosti, v souvislosti s trestním řízením a v souvislosti se zajišťováním krátkodobé ochrany osoby oprávněn používat podpůrné operativně pátrací prostředky, kterými jsou

a) *informátor*
b) *krycí prostředky*
c) *zabezpečovací technika*
d) *zvláštní finanční prostředky*[11]

Vzhledem k vyšetřované problematice podvodů, je užití podpůrných operativně pátracích prostředků velmi omezeno. Z vyjmenovaných podpůrných operativně pátracích prostředků přicházejí v úvahu ve výjimečných případech zvláštní finanční prostředky podle §77 z. č. 273/2008 Sb., o Policii České republiky, v posledním znění a zabezpečovací technika podle §76 z. č. 273/2008 Sb., o

[11] Zákon č. 273/2008 Sb., o Policii České republiky v posledním znění.

Policii České republiky, v posledním znění. Použití informátora podle §73 z. č. 273/2008 Sb., o Policii České republiky je využíváno velmi vzácně, vzhledem k tomu, že vyšetřovaná trestná činnost podvodů a v poslední době hlavně internetových podvodů, se nekoná nikde na veřejných prostorech, ale tuto trestnou činnost páchají jedinci nebo malé uzavřené skupiny v domácnostech nebo pronajatých kancelářích. V takovém případě získání informátora je velmi obtížné a je zde vysoké riziko prozrazení vyšetřování pachatelům. Užití krycích prostředků podle §74 z. č. 273/2008 Sb., o Policii České republiky se při vyšetřování podvodů až na výjimky nevyužívá, kdy k výše uvedenému pro tento podpůrně operativně pátrací prostředek není využití, ani možnost jeho nasazení.

6.2 Operativně pátrací prostředky

PČR užívá při vyšetřování trestných činů dále operativně pátrací prostředky, které jsou řízeny podle zákona 141/1961 Sb., o trestním řízení soudním, v posledním znění. Podle uvedeného zákona § 158c operativně pátracími prostředky jsou

a) *předstíraný převod*
b) *sledování osob a věcí*
c) *použití agenta*

6.2.1 Předstíraný převod

Předstíraným převodem se rozumí předstírání koupě, prodeje nebo jiného způsobu převodu předmětu plnění včetně převodu věci,

a) *k jejímuž držení je třeba zvláštního povolení,*
b) *jejíž držení je nepřípustné,*
c) *která pochází z trestného činu nebo*
d) *která je určena ke spáchání trestného činu.*[12]

Předstíraný převod se při vyšetřování podvodů a úvěrových podvodů až na velmi vzácné výjimky nevyužívá. Vzhledem k výše uvedenému paragrafovému znění a k tomu, že cílem útoku pachatelů při páchání trestných činů podvod a úvěrový

[12] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění.

podvod jsou finanční prostředky poškozených, není možnost předstíraný převod použít.

6.2.2 Použití agenta

Agentem je příslušník Policie České republiky nebo Generální inspekce bezpečnostních sborů plnící úkoly uložené mu řídícím policejním orgánem, vystupující zpravidla se zastíráním skutečného účelu své činnosti. Je-li to k použití agenta, jeho přípravě nebo k jeho ochraně nutné, je k zastírání jeho totožnosti možné

a) *vytvořit legendu o jiné osobní existenci a osobní údaje vyplývající z této legendy zavést do informačních systémů provozovaných podle zvláštních zákonů,*
b) *provádět hospodářské činnosti, k jejichž vykonávání je třeba zvláštní oprávnění, povolení či registrace,*
c) *zastírat příslušnost k Policii České republiky nebo ke Generální inspekci bezpečnostních sborů.*[13]

Použití agenta při vyšetřování podvodů a úvěrových podvodů je povětšinou vyloučené z podstaty průběhu páchání trestných činů podvodů a doprovodné trestné činnosti. Vzhledem k tomu, že pachatelé a organizované skupiny páchají svou trestnou činnost takzvaně za zavřenými dveřmi. Ve značné míře se jedná o malé skupiny pachatelů, kteří nepřicházejí do styku s běžným podsvětím, je tak nasazení agenta prakticky nemožné

6.2.3 Sledování osob a věcí

Sledováním osob a věcí (dále jen "sledování") se rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky. Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.[14]

[13] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění.
[14] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění.

Sledování osob a věcí je z operativně pátracích prostředků nejpoužívanější. Nejčastěji je používáno pro zjištění a případné ztotožnění všech členů organizované skupiny, protože členové těchto skupin zpravidla operují s jasně rozdílnými zaměřeními. PČR se ve většině případů podaří zjistit totožnost pachatelů, kteří buď přímo komunikují s poškozenými prostřednictvím telefonu nebo internetové aplikace, anebo se PČR podaří zjistit totožnost pachatelů, kteří pracují se získanými finančními prostředky. Členové těchto organizovaných skupin mívají i další zaměření z vnějšího pohledu skryté, jako je například získávání SIM karet, nových telefonů nebo získávání osobních údajů budoucích poškozených. Při sledování osob a věcí se smí zasahovat do nedotknutelnosti obydlí, narušit listinné tajemství nebo jiného obsahu komunikace pouze s povolením soudce. Obrazové a zvukové záznamy se smí pořizovat pouze se souhlasem státního zástupce.

6.3 Odposlech a záznam telekomunikačního provozu

Odposlech a záznam telekomunikačního provozu je upraven v zákoně číslo 141/1961 Sb., o trestním řízení soudním v posledním znění a to v §88 a v §88a. V paragrafu 88a zákona č. 141/1961 Sb., o trestním řízení soudním je trestný čin podvodu podle § 209 z. č. 40/2009 Sb., trestního zákoníku, v posledním znění jedním z vyjmenovaných trestných činů u kterých *"je-li to třeba pro účely trestního řízení, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství a nebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené".*[15] Jedná se o zdaleka nejužívanější nástroj při vyšetřování podvodů a úvěrových podvodů a trestných činů s tím souvisejících, i když v poslední době je z důvodu rozvoje nových technologií patrný ústup užívání tohoto nástroje. Odposlech a záznam telekomunikačního hovoru je možné pouze mezi dvěma stanicemi, které užívají pro přenos hovorů klasické GSM spojení mobilního operátora (klasický hlasový hovor) nebo zprávy formou běžných SMS a MMS. V dnešní době, pokud pachatelé užívají ke komunikaci nějaký internetový nástroj, popřípadě i hlasové volání cestou aplikace třetí strany,

[15] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění.

která komunikuje přes datové spojení mobilního operátora, není možné takto prováděné hovory odposlechnout a zaznamenat. Vzhledem k fungování datového spojení mobilního operátora, není známa ani cílová stanice takto provedených hovorů. Při prováděném odposlechu a záznamu telekomunikačního provozu, je pak tento hovor zaznamenán pouze jako datový provoz a jeho obsah a cíl komunikace je nedostupný pro PČR i pro mobilního operátora. Dalším limitem užívání odposlechu a záznamu telekomunikačního provozu je limitní doba, po kterou mobilní operátoři povinně ukládají data o mobilním a internetovém provozu, a to pouze po dobu 6 měsíců nazpět. Po uplynutí této lhůty již není možné získat žádný záznam o uskutečněném telekomunikačním provozu.

Záznam telekomunikačního provozu se dále užívá pro zjištění IP adres, ze kterých pachatelé komunikovali s poškozeným nebo ke zjištění IP adresy ze kterých probíhal útok na internetové služby 3. stran, a to buď formou softwarového útoku nebo formou podvodně získaných přihlašovacích údajů poškozeného.

6.4 Mezinárodní justiční spolupráce v trestních věcech a Evropský vyšetřovací příkaz

Při vyšetřování podvodů a úvěrových podvodů se velmi často PČR spoléhá na Mezinárodní justiční spolupráci v trestních věcech a Evropský vyšetřovací příkaz. vzhledem k tomu, že valná většina zmíněných trestných činů se v dnešní době páchá prostřednictvím internetové sítě, není výjimkou že na občany ČR nebo na cizince žijící na území ČR, jsou prováděny útoky ze zahraničí. PČR se tak v těchto případech spoléhá na Mezinárodní justiční spolupráci v trestních věcech, anebo na Evropský vyšetřovací příkaz. V obou případech při zjišťování majitelů bankovních účtů, při zjišťování uživatelů IP adres zjištěných během vyšetřování a v neposlední řadě v ověření zjištěných totožností, zdali zjištěná osoba existuje nebo se jedná o podvržené osobní informace, a další. Nevýhodou Mezinárodní justiční spolupráce v trestních věcech je doba od vydání podnětu státnímu zástupci k vydání žádosti o mezinárodní právní spolupráci po obdržení výsledku dožádání. Dalším limitujícím faktorem jsou samotné mezinárodní smlouvy, které má uzavřená Česká republika se státy mimo Evropskou unii, ke kterým je žádost směřována. Pokud jde o Evropský vyšetřovací příkaz, ten je z hlediska časové

náročnosti mnohem rychlejší, i když se bavíme o lhůtě zhruba 3 až 6 měsíců. Výhodou Evropského vyšetřovacího příkazu je, že státy Evropské unie mají jednotné formuláře na Evropský vyšetřovací příkaz, na které státy Evropské unie odpovídají v celku jednotně. Jedná se o zavedený systém.

6.5 Součinnost státních orgánů, fyzických a právnických osob

K vyšetřování trestných činů užívá PČR také součinnosti s fyzickými a právnickými osobami. Ve většině případů se jedná o získání záznamů právnických osob poskytujících bankovní a nebankovní služby a internetové služby. Při dožadování informací od soukromých a právnických osob postupuje PČR v souladu s § 8 odst. 1 z. č. 141/1961 Sb., trestního řádu v posledním znění.

Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin.[16]

PČR zpravidla požaduje informace o připojení ke službám, které poskytuje daná právnická osoba. Nejčastěji se jedná o poskytovatele free mailových služeb, chatovacích služeb a cestou Evropského vyšetřovacího příkazu nebo Mezinárodní justiční spolupráce také poskytovatele sociálních sítí. Jedná se o zjištění IP adres, přesných časů připojení a registračních údajů. Při vyšetřování zejména úvěrových podvodů jsou často vyžadovány informace od Nebankovního registru klientských informací (CNCB Czech Non-Banking Credit Bureau, z.s.p.o.), který shromažďuje informace o klientech leasingových a úvěrových společností.

PČR při vyšetřování podvodů a úvěrových podvodů při získávání informaci od bankovních institucí postupuje podle §8 odst. 2) z. č. 141/1961 Sb., o trestním řízení soudním v posledním znění, podle kterého mimo jiné lze v odůvodněných případech, cestou státního zastupitelství vyžádat informace, které jsou předmětem bankovního tajemství. Od bankovních institucí je možné zjistit pohyb

[16] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění.

finančních prostředků, cílové účty, výpisy z účtů, zjistit informace o platebních kartách, kdy a kde byly použity, zdali proběhl nějaký výběr z bankomatu, kdy a kde. Dále je možné zjistit přístupy do internetového bankovnictví včetně IP adres, které do internetového bankovnictví přistupovaly a v jakém čase, lze zjistit majitele a disponenta účtu, majitelé platební karty a registrační údaje majitele účtu. Obdobné informace lze zjistit také u úvěrových služeb bankovních institucí, které banka poskytla nebo úvěrů o které bylo zažádáno. Od bankovních institucí je možné dále zjistit kopie dokladů a dalších listin které majitel účtu předložil při zakládání účtu nebo při žádosti o úvěr. Podle uvedeného paragrafu lze také dožadovat informace u Bankovního registru klientských informací (CBCB – Czech Banking Credit Bureau, a. s.), který obsahuje informace o úvěrových smlouvách mezi klienty a bankami.

7 Aktuální problémy během vyšetřování

Aktuální problémy během vyšetřování podvodů a její doprovodné trestné činnosti nejvíce vyplývají s rozvojem nových technologií a možností komunikace. Jak již bylo popsáno výše, pachatelé aktuálně páchaných podvodů a doprovodné trestné činnosti mají k dispozici nespočet nástrojů, které jim usnadňují páchání trestné činnosti, ztěžují orgánům činným v trestním řízení vyšetřování, omezují nebo přímo znemožňují zjištění totožnosti pachatelů. Pachatelé páchající aktuální trestnou činnost za využití moderních technologií, mají vždy výhodu náskoku před orgány činnými v trestním řízení, které pouze mohou reagovat na vzniklou situaci a nové způsoby páchání trestné činnosti.

7.1 Nezjištěné místo činu

Mezi základní problémy, které provázejí vyšetřování podvodů a doprovodné trestné činnosti, se kterými se musí orgány činné v trestním řízení vypořádat, patří i po nahlášení trestného činu nezjištěné místo činu. Zpravidla při vyšetřování podvodů a doprovodné test činnosti je známé pouze místo následku a poškozený, není výjimkou, že místo činu se nenachází na území České republiky. To má za následek již od počátku trestního řízení velký nedostatek důkazního materiálu. Během aktuálně páchané trestné činnosti pachatelé velmi často využívají služeb VPN a sítě TOR. Proto zjištěné informace cestou dožádání k fyzickým nebo

právnickým osobám, případně bankovním institucím nebo cestou Evropského vyšetřovacího příkazu a mezinárodní justiční spolupráce, kdy zjištěnými informacemi jsou zpravidla IP adresa, ze které docházelo k připojení k napadeným službám nebo komunikaci s poškozeným, je pouze adresa serveru poskytovatele VPN nebo výchozí server ze sítě TOR. Tedy zcela neupotřebitelné informace. Je zjištěno že pachatelé, kteří používají internetové komunikační nástroje komunikují šifrovaně, a to i s koncovými uživateli z podvržených telefonních čísel, kdy telefonní hovor je přesměrován i přes několik států v Evropské unii nebo i mimo ni. Vzhledem k výše uvedenému se velmi často nepodaří zjistit místo činu.

7.2 Nedostatek fyzických důkazů

Dalším aktuálním problémem při vyšetřování podvodů a další doprovodné trestné činnosti, který souvisí se zmíněným problémem nezjištěného místa činu. Je to nedostatek fyzických důkazů. Vzhledem k tomu, že není zjištěno místo činu, nelze získat žádné fyzické důkazy ani výpočetní techniku ohledáním při začátku a velmi často i během vyšetřování. Během vyšetřování je k dispozici jen malá skupina elektronických stop. Bývá to kopie komunikace poškozeného s pachatelem, IP adresa a telefonní číslo. Další mohu být číslo bankovního účtu pachatele nebo název krypto peněženky pachatele. Pokud jde o získávání fyzických důkazů a jejich vyhodnocování, k tomu zpravidla dochází až poté, co byl zjištěn pachatel dané trestné činnosti a byl soudem vydán příkaz k domovní a nebytové prohlídce, kde je poté možné zajistit výpočetní techniku, záznamová zařízení, mobilní telefony, SIM karty a popřípadě dokumentaci. Pak zpravidla dochází k dlouhému znaleckému zkoumání zajištěné elektroniky. Výsledkem takovýchto znaleckých zkoumání je zpravidla výstup se zajištěnými elektronickými soubory v řádech desetitisíců. Poté musí policisté každý jednotlivý soubor otevřít a zkontrolovat, zdali se takovýto soubor týká vyšetřované trestné činnosti, zadali je upotřebitelný a do záznamu každý jednotlivý upotřebitelný soubor popsat a spojit s vyšetřovanou trestnou činností. Nejvíce se jedná o běžné typy souborů jako obrazové soubory (.png, .jpg. apod.), soubory kancelářských aplikací, tabulky, textové soubory (.doc, .docx, .xlx, .xlsx, .pdf, .txt apod.) a v neposlední řadě zajištěné kontaktní údaje, které měl pachatel uloženy. V takto zajištěných souborech bývají zjištěné fotografie osobních dokladů poškozených, falzifikáty

písemností v různých stádiích dokončení, podvržená razítka v různých stadiích dokončením, záznamy s přístupovými údaji do různých internetových služeb, které pachatelé užívali, odcizili nebo podvodně založili na poškozené a hlavně záznamy s přístupovými údaji, k bankovním účtům ať už svým nebo přístupové údaje k bankovním účtům které podvodně založili na poškozené. V zajištěných mobilních telefonech se často nachází stejný vzorek souborů jako v počítačích, s tou výjimkou, že v mobilních telefonech se často nachází zálohy z komunikačních aplikací, které pachatelé užívali, historie hovorů a kontakty, které měli pachatelé uloženy. Po vyhodnocení takto zajištěných stop je častým úkazem další rozšíření trestního stíhání pachatelů o skutky, které nebyly doposud s trestnou činností pachatelů spojovány. Příkladem byla zjištěna další telefonní čísla nebo e-mailové schránky, které pachatelé užívali a které byly užity v jiné trestné činnost, kterou PČR vyšetřuje na jiném oddělení nebo v jiném územním celku. Tato situace velmi ztěžuje vyšetřování, protože od počátku vyšetřování a během vyšetřování je nejvíce důkazů pouze elektronických a často nepřímých, případně paměťových stop od poškozených, které, vzhledem k tomu, že pachatele poškození nikdy neviděli, maximálně se s ním telefonovali, moc upotřebitelných informací nepřináší. Většinou je to pouze zjištěné pohlaví, národnost, a odhadnutý věk pachatele.

7.3 Časová prodleva

Velmi častým problémem při vyšetřování podvodů a její doprovodné činnosti je také časová prodleva od spáchání trestného činu po jeho nahlášení. Toto se týká hlavně právnických osob, zejména úvěrových společností, které postupují dle zásady subsidiarity trestní represe. Pokud se podaří pachateli získat neoprávněně úvěr u úvěrové společnosti na neexistující totožnost nebo na totožnost osoby, jejíž osobní údaje získal jiným způsobem a neoprávněně použil při žádosti o úvěr, dochází často k veliké prodlevě. Takovéto úvěrové společnosti se dle svých vlastních smluvních podmínek snaží smyšleného dlužníka nejdříve kontaktovat poštou a jinými obdobnými způsoby. Poté, kdy toto snažení je zcela marné, podává úvěrová společnost k soudu návrh na zahájení exekučního řízení, kde se zjistí, že dlužník fakticky neexistuje, anebo osoba, na kterou byl podvodně zřízen úvěr, se teprve dozví, že její osobní údaje byly zneužity. Další možností, kdy

dochází k výrazné časové prodlevě je v případech, kdy pachatel získá osobní údaje svého rodinného příslušníka nebo kamaráda, které poté použije k uzavření úvěrové smlouvy, ale úvěr řádně splácí. To, že byl spáchán úvěrový podvod, je pak nejčastěji zjištěno tak, že poškozený, od kterého byly odcizeny osobní údaje, si chce sám požádat o úvěr nebo o hypotéku. Ten pak ve své bance nebo úvěrové společnosti zjistí, že je veden jako dlužník a úvěr nebo hypotéka mu není poskytnuta. Vzhledem k výše uvedenému a možné značné časové prodlevě, která může být ve výjimečných případech i delší než rok, má pak PČR při vyšetřování omezené možnosti. Jak již bylo popsáno výše, provozovatelé telekomunikačních služeb v ČR jsou povinni zachovávat záznamy o uskutečněném telekomunikačním provozu po dobu 6 měsíců. Vzhledem k tak velké časové prodlevě si svědkové nic nepamatují a poradci, kteří mohli smlouvy dojednávat, už nemusí být u úvěrových společností ani zaměstnáni.

7.4 Neexistence důkazního materiálu

Další problémem během vyšetřování je faktická neexistence důkazního materiálu. Jedná se hlavně o neexistenci důkazního materiálu v elektronické podobě, kdy pachatelé správně užili výše popsané nástroje pro maskování své totožnosti Pokud pachatele správně použijí nástroje jako je služba VPN nebo síť TOR a dále správně užijí kryptoměny a sociální inženýrství, důkazní materiál neexistuje. Pokud jde o důkazní materiál ve formě záznamu komunikačního provozu, tak při správném použití VPN nebo sítě TOR jsou zjištěné IP adresy od poškozeného nebo zasažené společnosti pouze servery poskytovatelů služeb VPN nebo servery výchozích bodů ze sítě TOR, které neukládají žádné záznamy o internetovém provozu i vzhledem k tomu, že veškerá komunikace, která přesně prochází je šifrovaná. V takovémto případě, pokud se zjistí provozovatel služby VPN, ani on sám nemá žádná data, která by mohl policii poskytnout. Dalším nástrojem, který pachatelé pak používají pro praní získaných finančních prostředků jsou kryptoměny. Správným použitím kryptoměn je jejich trasování téměř nemožné. Pokud dojde k převodu na kryptoměnu MONERO je trasování nemožné zcela. Pokud pachatel využije všech výhod komunikačních nástrojů jako je WhatsApp, není výjimkou, že pachatel telefonuje jednomu poškozenému přes hovor komunikátoru WhatsApp z telefonního čísla s předčíslím Velké Británie o

hodinu později ten samý pachatel volá z telefonního čísla s předčíslím Rakouska a následně třeba z Ruské federace. Pokud tento internetový hovor byl provozován přes síť TOR nebo službu VPN, je jeho dohledání nemožné.

7.5 Neexistence hranic v online prostoru

Dalším z hlavních problému, se kterým se musí PČR vypořádat je neexistence hranic v online prostoru. Internetová síť značně rozšiřuje možný dosah pachatelů, který tak není omezen jenom územím, kam se může pachatel fyzicky dostat, ale jeho dosah je prakticky neomezený ve všech zemích, ve kterých je internetové připojení. Pokud je pachatel svým jednáním (např. pro jazykovou bariéru) omezený pouze na území České republiky, není výjimkou, že poškození v jedné řadě trestných činů jsou rozmístěni po celém území České republiky. Příkladem je možné uvést klasický internetový podvod s falešným inzerátem na inzertním webovém portálu, kdy pachatel přijímá platby předem, ale slibované zboží nikdy neodešle. Na jeden takovýto inzerát mohu odpovídat lidé z celé České republiky, není výjimkou, že na takovýto inzerát zareagují i občané Slovenské republiky na jejich území. Připojení k internetu otevírá pachateli přístup k velké skupině potenciálních poškozených rozmístěných po celé České republice, respektive po celém světě. Nastalá situace tak mění základní principy, jak doposud PČR pracovala. PČR je rozdělena na územní celky, mimo oddělení s celorepublikovou působností. V každém územním celku potom dané oddělení působí v rámci své problematiky. Nastalá situace pak PČR stěžuje spojení jednotlivých skutků v sérii, kdy je problém na základě běžných atributů pospojovat jednotlivé trestné činy k určitému pachateli a k určité sérii trestných činů. S tím nastávají další administrativní problémy, jako je třeba řádný výslech poškozených, kteří jsou rozmístěni po celém území ČR a následné ztížení akumulace důkazního materiálu na jednom oddělení. Vyšetřování se tak prodlužuje po dobu nezbytně nutnou k postupování spisových materiálů po území ČR nebo po dobu nutnou k provedení dožadovaných výslechů poškozených na území ČR. Internetová kriminalita zvyšuje nároky na policisty, pokud jde o správné vyplňování položek do systému ETŘ, správný a věcný popis skutku. Dále to zvyšuje administrativní nároky na policistů při vytěžování systému ETŘ a dalších informačních systémů.

7.6 Přestupkové jednání

Oznámení, které přijímají základní útvary PČR od poškozených jsou velmi často kvalifikovány jako pouhý přestupek, zejména kdy se jedná o nedoručení bazarového zboží. V takovýchto případech se jedná o škody v řádech jednotek tisíců korun českých. Takto kvalifikované přestupkové jednání často končí bez hlubšího prověřování, i když se může jednat o dílčí skutek celé série, kterých se dopustila jediná osoba, následně se škodou přesahující desítky tisíc korun českých.

7.7 Nevzdělanost obecné populace v IT

Posledním a nejpalčivějším problémem při vyšetřování aktuálně páchaných podvodů a jejich doprovodných trestných činů, je obecná nevzdělanost populace v oblasti IT. To je patrné už při prvotním výslechu při příjmu oznámení, kdy poškozený zpravidla neví, jaké má doma nastavení modemu, jaké má zřízené internetové připojení, neumí si správně zabezpečit své účty na internetu nebo svůj vlastní počítač. Pachatelé, kteří v posledních letech páchají podvodnou trestnou činnost na internetu již dávno zjistili, že nejslabším článkem jakéhokoliv IT zabezpečení je právě uživatel. Většina populace v ČR jsou běžní uživatelé počítačových systému, kteří se nevzdělávají ve fungování počítačových systémů, ani v nových možnostech zabezpečení nebo v nových hrozbách, které jim hrozí. Z pohledu PČR je běžný uživatel schopen pracovat na počítači tak, že jej využívá, umí surfovat po internetu, přihlásit se do svých služeb nebo si nové hrubě založit. Ne však již řádně nastavit. Takovýto uživatel není pak schopen hlouběji pracovat v systému na svém počítači, není schopen si nastavit vyšší zabezpečení jak na svém počítači nebo internetovém připojení, případně internetové službě. Většina uživatelů neužívá žádné další zabezpečení než běžně dostupné antiviry.

7.7.1 Neznalost běžného zabezpečení

S nevzdělaností obecné populace v používání IT systému je pak často sledována vysoká důvěřivost těchto uživatelů, kteří slepě následují pokyny pachatelů na telefonu nebo formou e-mailových zpráv a sami uživatelé si do počítače nainstaluji škodlivý software, anebo software pro vzdálené ovládání počítače, aniž by si uvědomovali, že tak zpřístupňují celý svůj systém pachateli. Takovýto důvěřiví

uživatelé si informace, které obdrželi od někoho, koho ani nikdy neviděli a nikdy o něm před tím neslyšeli, nijak ověřili na internetu nebo u známých. Není výjimkou, že software pro vzdálené ovládání počítače je nainstalován na účtu správce počítače s administrátorskými oprávněními.

Většina dnešních moderních internetových služeb nabízí dvou faktorové zabezpečení ať už ve formě SMS zpráv s číselným kódem nebo plovoucím číselným kódem u autentifikátorské aplikace, která bývá nejčastěji nainstalovaná v mobilním telefonu. Dalším příkladem může být biometrické ověření buď v systémech mobilních telefonů nebo i na počítačích, a to ať už se systémem iOS nebo Windows. Z vyjmenovaných je zabezpečení formu SMS zpráv jedním z nejslabších, protože i přes v celku běžné varování, že kód obsažený v SMS zprávě by uživatel neměl nikdy nikomu předávat, se to velmi často děje. Největší výhodou dvou faktorového zabezpečení je, že obejít dvou faktorové zabezpečení pachatelem bez aktivní spoluúčasti poškozeného je velmi složité i z technického hlediska. Pokud dojde prolomení dvou faktorového zabezpečení pachatelem do internetové služby, zpravidla k tomu dochází formou formulářů pro zapomenuté přihlašovací údaje, kdy uživatel již provedl špatné úvodní nastavení zabezpečení svého účtu.

Dalším z běžných způsobů, se kterými dochází k odcizení například Free mailového účtu nebo účtu do sociální sítě, je užívání stále se opakujícího stejného jednoduchého hesla u všech služeb, které má daný uživatel zřízeny na internetu, bez aktivovaného dvou faktorového zabezpečení. Poté stačí jediný unik informací na jediné ze služeb uživatele, což není nic výjimečného a pachatelé tak získají přihlašovací údaje ke všem možným službám poškozeného. Pachatelé poté využívají automatizovaných systémů, které samy zadávají získané přihlašovací údaje do různých služeb na internetu s vysokou úspěšností a rychlostí. Databáze uniklých přihlašovacích údajů a uniklých údajů o platebních kartách, jsou běžně dostupné k nákupu na Dark Webu. V některých případech jsou databáze i ověřené, kdy prodávající garantuje určitou procentuální úspěšnost nabízených údajů platebních karet, anebo přihlašovacích údajů poškozených. Toto je často při výslechu poškozeného vysvětlováno tím, že si nikdo nemůže pamatovat takové množství různých složitých hesel pro každou službu zvlášť. Přitom jednoduchým

řešením takovéhoto problému je obyčejný správce hesel. Správců hesel je dnes k dispozici spousta, některé jsou i zcela zdarma a jsou schopné fungovat na všech operačních systémech, včetně na operačních systémech mobilních telefonů.

7.8 Nevzdělanost policistů v IT a nevybavenost PČR

Jedním ze základních problémů, které zdržují vyšetřování je nevzdělanost běžných policistů na obvodních odděleních a místních oddělení policie v IT problematice jako takové. Úvodní výpovědi poškozených, které poškození učinili při nahlašování trestných činů, jsou velmi často shledány jako nedostatečné. Nejsou zodpovězeny potřebné otázky, které jsou základní pro další směřování vyšetřování. Postupem času, je ale zjevný posun k lepšímu při úvodních výsleších, kdy policisté na obvodních a místní oddělení policie si zlepšují své znalosti v oblasti IT a jejich zkušenosti se stále častějším příjmem oznámení v oblasti IT kriminality se neustále rozšiřují.

To umocňuje další problém, se kterým se policie v oblasti IT kriminality potýká, a to je nedostatek školení. Policie nezajišťuje dostatečné školení v oblastech IT kriminality pro běžné policisty ani pro policisty na Službě kriminální policie a vyšetřování (SKPV). Znalosti, které jsou potřebné pro příjem oznámení a další vyšetřování takovéto kriminality policisté často musí sami získat samostudiem, někdy i ze zahraničních zdrojů. Přitom základní porozumění fungování IT systémů ať už počítačů, počítačových sítí nebo mobilních telefonů a mobilních sítí jsou naprostou nezbytností pro vyšetřování IT kriminality a podvodů páchaných v kyberprostoru.

Další problém policie, který zdržuje a ztěžuje vyšetřování podvodů, je nedostatek programového vybavení na útvarech policie. Běžné služební počítače připojené k systému ETŘ neobsahují žádné analytické nástroje, žádné programové vybavení na strojové čtení, žádné programové vybavení na převod formátu souborů. Tento nedostatek programového vybavení ve služebních počítačích nutí policisty, kteří vyhodnocují stopy zajištěné u pachatelů procházet jednotlivé soubory zvlášť a ručně. Ruční vyhodnocování takovýchto stop, kde se počty souborů, které se musí prověřit šplhají do řádů desetitisíců, velmi zdržuje vyšetřování. Není výjimkou, že běžný služební počítač nemá ani dostatečnou

kapacitu paměti pro uložení digitálních stop z jednoho případu najednou. V této problematice spatřujeme jeden další problém, a to jsou omezené přístupy policistů zařazených na vyšetřování podvodů a IT kriminality do dalších systémů policie. Tyto omezené přístupy do policejních systému nutí takovéto policisty velmi často spolupracovat s oddělením analytiky, což oddělení analytiky značně přetěžuje i vzhledem k nárůstu kriminality a celé vyšetřování to značně zdržuje.

8 Příkladový trestný čin

Následující série trestných činů byla vyšetřována 6. Oddělením obecné kriminality (6.OOK), Služby kriminální policie a vyšetřovaní (SKPV), Krajského ředitelství policie hlavního města Prahy (KŘP hl. m. Praha), Obvodního ředitelství policie Praha II (OŘP PII). Vyšetřování se autor práce aktivně účastnil. V průběhu vyšetřování byl celý spisový materiál na pokyn státního zástupce postoupen Odbor obecné kriminality, 2. oddělení obecné kriminality, KŘP Praha. Vyšetřování probíhalo od listopadu roku 2018 do ledna 2022. Vzhledem k velké komplexnosti vyšetřovaného případu, je popis případu a vyšetřování značně zjednodušen.

Vyšetřováním byly zjištěni dva hlavní pachatelé. Pro účely bakalářské práce bude první z nich pojmenovaná pachatel „A“ a druhý pachatel „B“. Vyšetřovaní bylo zahájeno po oznámení od úvěrové společnosti, které obsahovalo několik úvěrových smluv, u kterých úvěrová společnost zjistila, že osoby, kterým vyplatila úvěry, neexistují. To zjistila společnost po tom, co po nepodařeném kontaktování dlužníků podala k soudu návrh na zahájení exekučního řízení.

Prověřováním oznámení bylo zjištěno, že na úvěrových smlouvách v pozici úvěrového poradce se opakují často jméno dvou úvěrových poradců, a to jméno pachatele „A“ a pachatele „B“. Dalším šetřením bylo zjištěno, že u jedné úvěrové smlouvy byly finanční prostředky zaslány na bankovní účet pachatele „B“. Byly vyžádány další úvěrové smlouvy, které zpracovávali uvedení pachatelé. Bylo zjištěno, že u spousty smluv je zaregistrováno splácení úvěru jen v několika prvních splátkách. Dále bylo zjištěno, že uvedení pachatelé již nejsou zaměstnanci úvěrové společnosti, kdy oba podali výpověď.

Podle § 8 odst. 2) z. č. 141/1961 Sb., trestního řádu, byly cestou státního zástupce získány výpisy z bankovních účtů obou pachatelů, ve kterých bylo zjištěno, že ač

ani jeden z nich není zaměstnán oba disponují značnými finančními prostředky, které přicházely na jejich účty z od různých soukromých osob. Z bankovních výpisů bylo mino jiné zjištěno, že pachatel „A“ platí za nájem kanceláře, na Praze 5. Do protější budovy od budovy, kde se nacházely kanceláře (shodou okolností objekt PČR) byl naistalován kamerový systém podle § 72 a §76 z. č. 273/2008 Sb., o Policii České republiky. Ze záběrů zachycených kamerovým systéme byly zjištěny vozidla, se kterými se pachatelé pohybuji, stejně jako byly zjištěni další spolupachatelé. Byly zjištěni další pachatelé a to pachatel „C“, „D“, „E“, “F“, “G“. Dále byla ustanovena vozidla, se kterými se zjištění pachatelé pohybovali.

Dalším šetřením kolem bankovních výpisů byly zjištěny jména odesílatelů finančních prostředků oběma hlavním pachatelům. Šetřením v systémech policie byly z této skupiny lidí zjištěni oznamovatelé, kteří zjistili, že je na jejich totožnost vedeno několik nebankovních půjček, které sami nezakládali a celou situaci nahlásili na místně příslušném obvodním oddělení policie (OOP). Bylo zjištěno, že poškození se nacházejí rozmístěni po celé ČR. Spisové materiály oznamovatelů těchto oznámení byly vyžádány a následujícími výslechy bylo zjištěno, že všichni oznamovatelé mají společnou jednu věc. Všichni odpovídali na internetový inzerát nabízející zaměstnání. Při komunikaci se společností, která nabízela zaměstnání, poškození vždy zaslali fotokopie svých osobních dokladů. Následně byli poškození požádání společností nabízející zaměstnání, aby zaslali 1,-Kč bankovním převodem na společností určený bankovní účet. Údajně pro ověření totožnosti žadatelů o zaměstnání.

Prověřením podvodných úvěrových smluv na poškozené, bylo zjištěno, že tyto smlouvy obsahovaly fotokopie dokladů, které poškození zasílali společnosti nabízející zaměstnání. Zpětným prověřením bankovních výpisů, které poskytli poškození, bylo zjištěno, že v každém případě poškození nevědomky zasílali zjištěnou 1,-Kč na svůj nově vytvořený účet. Tak byla stanovena vyšetřovací verze, že pachatelé „A“ a „B“ takto pod záminkou nabídky zaměstnání získávají osobní doklady poškozených. Tyto doklady pak dále užívají k online zakládání bankovních účtů jménem poškozených a pod legendou ověření totožnosti, poškození nevědomky aktivují falešně založené bankovní účty. Ostatní pachatelé

zastávají podpůrnou roli a vydávají se za údajné zaměstnavatele poškozených při podvodném sjednávání úvěrových smluv.

Dalším prověřováním úvěrových smluv na poškozené a přiložené smluvní dokumentace, bylo zjištěno, že kontaktní údaje uvedené na smluvní dokumentaci nikdy nepatřily poškozeným. Jednalo se o e-mailové adresy, telefonní čísla a kontaktní adresy. Dále bylo zjištěno, že bankovní výpisy a výplatní pásky nepatří poškozeným, a prověřením skutečných bankovních výpisů podle uvedených bankovních účtů bylo zjištěno, že tyto jsou podvrženy. Společnosti na výplatních páskách jsou povětšinou smyšlené, popřípadě uvedená telefonní čísla nepatří uvedeným firmám. Šetřením v systémech policie a ve spolupráci s Útvarem zvláštních činností služby kriminální police a vyšetřování (ÚZČ), bylo podle IMEI mobilních telefonů zjištěno, že některá telefonní čísla z podvodných smluv, a to buď telefonní čísla, která byla uvedená jako kontaktní na klienta úvěrové společnosti nebo jako kontaktní na zaměstnavatele klienta úvěrové společnosti. Byly vloženy do mobilních telefonů pachatele „A“ a pachatele „B“ a několika dalších, ve kterých jsou běžně vloženy SIM karty vedené na jejich jména. Do této doby byla zjištěna celková škoda cca 1.200.000, - Kč.

Proto byl vydán podle § 88 odst. 1 z. č. 141/1961 Sb., trestního řádu podmět státnímu zástupci na vydání návrhu k soudu na vydání příkazu k odposlechu a záznamu telekomunikačního provozu. Soud návrhu státního zástupce vyhověl. Během probíhajících odposlechů nebyl zjištěn, žádný poznatek upotřebitelný pro trestní řízení. Pokaždé, když pachatelé začínali mluvit o svém „zaměstnání“, pachatel „A“ vždy navrhl, aby hovor pokračoval přes WhatsApp nebo Messenger. Vzhledem k tomu, že odposlech a záznam telekomunikačního provozu nepřinášel žádné upotřebitelné informace, byl končen.

Dalším šetřením u úvěrových společností na přítomnost zjištěných smyšlených společností a zjištěných telefonních čísel byly různě po území ČR zjištěny další úvěrové smlouvy u kterých nejsou spláceny žádné splátky nebo bylo zaplaceno několik prvních splátek, ale nyní jsou v prodlení. Dalším šetřením v systémech policie po zjištěných atributech, byly zjištěny další spisové materiály, které byly vyžádány a sloučeny ke společnému řízení. Dále byly od úvěrových společností zajištěny žádosti o poskytnutí úvěru. Bylo zjištěno, že veškeré IP adresy, které

byly užity u zakládání bankovních účtů, žádostí o úvěr probíhaly z totožné IP adresy, která náležela poskytovateli na adrese, kde pachatel „A“ pronajímal kancelář. Bylo jasné, že pachatelé, kteří prováděli zjištěnou trestnou činnost se nachází v některé kanceláři, ukrytí v podsíti poskytovatele internetu v kancelářské budově.

Podle § 8 odst. 2) z. č. 141/1961 Sb., trestního řádu, byly cestou státního zástupce vyžádány další bankovní výpisy obou pachatelů. Bylo zjištěno, že pachatel „A“ získané finanční prostředky zasílá na kryptoměnovou burzu a značnou část použil ke koupi luxusního vozidla (BMW 550i), pachatel „B“ zasílá finanční prostředky do hazardních her. Následně bylo zjištěno, že pachatel „A“ ukončil nájem kanceláře

Na základě zjištěných informací, byla naplánována realizace v bydlišti obou pachatelů zároveň. Podle § 83 z. č. 141/1961 Sb., trestního řádu byly soudem vydány příkazy k domovní prohlídce na byty obou pachatelů a podle § 83a z. č. 141/1961 Sb., trestního řádu byly vydány příkazy k prohlídce jiných prostor a pozemků, konkrétně na zjištěná vozidla, ve kterých se pachatelé pohybovali.

Realizace proběhla podle plánu, oba hlavní pachatelé byli zadrženi, domovní prohlídky proběhly podle plánu. Během obou domovních prohlídek byly zajištěny počítače obou pachatelů, několik mobilních telefonů, značné množství SIM karet a paměťových zařízení. Zajištěná elektronika byla odeslána na znalecké zkoumání. Znalec zajistil ze všech počítačů, mobilních telefonů a paměťových zařízení 56 Gb. různých souborů (přes 70 000 souborů). Velmi zdlouhavým prověřováním všech zajištěných souborů a jejich porovnáváním se zjištěnými skutečnostmi, a policejními systémy, byly zjištěny další obdobné skutky, které prozatím nebyly zjištěny, nahlášeny nebo byli již odloženy podle § 159a odst. 5 z. č. 141/1961 Sb., trestního řádu. V počítačích pachatelů byly zajištěny velké databáze totožností, které jak bylo později zjištěno, pachatelé zkopírovali ve svém bývalém zaměstnání, ve kterém pracovali jako úvěroví poradci. Prověřením spisového materiálu bylo zjištěno, že pachatelé se dopustili 88 skutků, způsobili škodu 4.141.967, - Kč. Pachatelům bylo předáno usnesení o zahájení trestního stíhání, kdy podle §160 odst. 1 z. č. 141/1961 Sb., trestního řádu bylo zahájeno trestní stíhání pachatelů „A“ a „B“ jako obviněných ze spáchání pokračujícího zločinu úvěrový podvod podle § 211 odst. 1, odst. 5, písm. c) z. č. 40/2009 Sb.,

trestního zákoníku, dílem dokonaným, dílem ve stádiu pokusu podle § 21 odst. 1 z. č. 40/2009 Sb., trestního zákoníku, spáchaného ve spolupachatelství podle § 23 z. č. 40/2009 Sb., trestního zákoníku , v jednočinném souběhu s přečinem poškození cizích práv podle §180 odst. 1 písm. a), z. č. 40/2009 Sb., trestního zákoníku, spáchaného ve spolupachatelství podle § 23 z. č. 40/2009 Sb., trestního zákoníku, pokračujícího zločinu podvodu podle § 209, odst. 1, odst. 4 písm. a), písm. d) z. č. 40/2009 Sb., trestního zákoníku, dílem dokonaným, dílem ve stádiu pokusu podle § 21 odst. 1 z. č. 40/2009 Sb., trestního zákoníku, spáchaného ve spolupachatelství podle § 23 z. č. 40/2009 Sb., trestního zákoníku , v jednočinném souběhu se zločinem padělání a pozměnění veřejné listiny podle § 348 odst. 1, odst. 2, písm. c), z. č. 40/2009 Sb., trestního zákoníku.

Celkem bylo obviněno 12 pachatelů, kteří způsobili celkovou škodu 4.141.967, - Kč, a byli obviněni z 88 skutků při kterých způsobili škodu 69 poškozeným soukromým a právnickým osobám.

9 Závěr

Tato bakalářská práce rozebírá aktuální problémy metodiky vyšetřování podvodů. V úvodu práce bylo rozpracováno, co se považuje za podvod, a to jak z hlediska běžného chápání, tak z hlediska zákona. Stejně tak byly uvedeny vybrané doprovodné trestné činy, které s sebou páchání podvodů běžně přináší. Pro vysvětlení aktuálních problému metodiky vyšetřování jsou v bakalářské práci rozvedeny nástroje, které pachatelé při páchání podvodů a doprovodné trestné činnosti běžně užívají. Jasně je v práci znázorněn trend posunu páchané trestné činnosti, zejména podvodů do kyberprostoru a zřejmý nárust této kriminality v posledních letech.

Práce ukazuje značnou tvořivost pachatelů podvodů, při adaptaci legitimních nástrojů, k páchání trestné činnosti. Pachatelům se daří pro své účely zneužívat vývoj v technologiích pro svůj prospěch. Vynalézavost pachatelů je dále umocněna vývojem nástrojů přímo určených k páchání trestné činnosti, které využívají aktuální trendy v komunikaci mezi lidmi i společnostmi. To ukazuje na nevýhodu, kterou je zatížena policie při vyšetřování podvodů, protože proaktivní akce policie jsou prakticky nereálné a policie je nucena pouze reagovat na vzniklou situaci a současné trendy v páchání podvodů.

V průběhu práce byly vysvětleny aktuální způsoby páchání trestné činnosti podvodů, které jasně ukázaly jednoduchost takového páchání, stejně jako zranitelnost běžné populace k takovýmto podvodům. Byly vysvětleny základní nástroje, které policie používá při vyšetřování podvodů a jejich limity. Dále bylo zjištěno, že vzhledem k nástrojům, znalostem, dostupným technologiím a limitujícím legislativním procesem pachatelé získávají nad policí značný technologický náskok. To nejen k novým způsobům páchání podvodů, ale hlavně pachatelé získali značný náskok v možnostech zastírání své podvodné činnosti a k úspěšnému zastírání své identity.

Ze zjištěného vyplívá, že největší problémy při vyšetřování podvodů přináší právě nové technologie a jejich pomalá adaptace mezi policisty i běžnou populaci. Pro zvýšení objasněnosti při vyšetřování podvodů, se bude muset policie přizpůsobit rychlému rozvoji technologií, hlavně nákupem potřebného programového

vybavení. S tím se váže další problém, a to je vzdělání policistů v technologiích. Pachatelé užívají při páchání specializované nástroje, ať už legitimní nebo přímo vytvořené za účelem páchání podvodů. Dokud nebudou mít policisté, kteří přicházejí do styku s vyšetřováním podvodů na obvodních odděleních nebo na SKPV povědomí o těchto nástrojích a možnostech jejich využití, není možné řádně provést ani základní podání vysvětlení s poškozeným.

Metodika vyšetřování podvodů je dynamicky se rozvíjející zaměření, kterému bude v budoucnosti připisována stále větší důležitost.

Seznam použité literatury

KONRÁD, Zdeněk et al. *KRIMINALISTIKA kriminalistická taktika a metodiky vyšetřování.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-547-0.

PORADA, Viktor a kol. *KRIMINALISTIKA Technické, forenzní a kybernetické aspekty.* 2. aktualizované a rozšířené vyd. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

ČÍRTKOVÁ, Ludmila et al. *Podvody zpronevěry machinace.* Praha: Armex Publishing, 2005. ISBN 80-86795-12-8.

CHMELÍK, Jan a kolektiv. *Rukověť kriminalistiky.* Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-36-9.

WEBER, Monika. Morfing – aktuální bezpečnostní výzva nejen pro kriminalisty. *Kriminalistický Sborník.* Praha, Tiskárna Ministerstva vnitra, 2021, roč LXV č.1, s. 64-71.

Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění.

Zákon č. 141/1961 Sb., *o trestním řízení soudním* v posledním znění.

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních v posledním znění.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů v posledním znění.

Nalus.usoud.cz: Vyhledávání rozhodnutí Ústavního soudu České republiky [online].

HOVORKA Jiří. Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc [online] 2017 [cit. 03. 01. 2022]. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/.

Nalus.usoud.cz: Vyhledávání rozhodnutí Ústavního soudu České republiky [online] Nález Ústavního soudu ze dne 7. 11. 2006, sp. zn. I. ÚS 631/05 [cit.

28.11.2021]. Dostupné z https://nalus.usoud.cz/Search/GetText.aspx?sz=1-631-05.

policie.cz: Kyberkriminalita [online]. [cit. 14. 12. 2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

plk. MORAVČÍK Ondřej. Kriminalita klesla o více než 16 procent! [online] 2021. [cit. 14. 12. 2021]. Dostupné z https://www.policie.cz/docDetail.aspx?docid=22588801&docType=ART.

plk. MORAVČÍK Ondřej. Vývoj registrované kriminality v roce 2021 [online] 21. 01. 2022. [cit 02. 02. 2022]. Dostupné z https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx.

e-bezpeci.cz: Statistika kybernetické kriminality za rok 2019 [online] 22. 1. 2020. [cit.16. 12. 2021] Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019.

surfshark.com: Surfshark Secure your digital life [online]. [Cit 30. 12. 2021]. Dostupné z: https://surfshark.com/.

Seznam použitých obrázků

Seznam použitých grafů

Seznam použitých tabulek