Případová studie kybernetického útoku

Bc. Jaroslav Hoferek

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jaroslav Hoferek**
Osobní číslo:	**L22487**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Případová studie kybernetického útoku**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Analyzujte současný stav kybernetické bezpečnosti se zaměřením na moderní kybernetické útoky.
3. Navrhněte detailní scénář vybraného kybernetického útoku.
4. Zpracujte návrh preventivních opatření vůči vybranému kybernetickému útoku.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking.* Second edition. Indianapolis. IN: Wiley, 2018. ISBN 978-1-119-43338-5.
2. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
3. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 26.4.2024

Jméno a příjmení studenta: Bc. Jaroslav Hoferek

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá oblastí kybernetické bezpečnosti, přičemž se zaměřuje na problematiku zranitelnosti uživatelů. Teoretická část je koncipována do třech částí, kdy úvodní část je věnována analýze současného stavu. Navazující část shrnuje oblast kybernetické bezpečnosti pro pochopení tohoto odvětví. Třetí část je zaměřena na hrozby v kybernetickém prostoru, se kterými se dnes můžeme nejčastěji setkat.

Praktická část je rozdělena na dvě části. V první části je podle scénáře proveden kybernetický útok pomocí infikovaného souboru. Celý postup provedení útoku je doprovázen popisem jednotlivých úkonů, které bylo třeba vykonat. Krom nastínění průběhu útoku z pohledu útočníka, je možné se detailněji seznámit s použitým nástrojem. Toho lze využít při analýze zranitelností pro účely řízení rizik. Druhá polovina praktické části je zaměřena na oblasti zabezpečení systému a rozpoznání phishingu, se kterými by měli být uživatelé seznámeni pro vyhnutí se nejen demonstrovanému typu útoku. Jako výstup práce jsou pak ve formě přílohy zpracovány školicí materiály, které by měly uživatele vést k bezpečnému zacházení se zařízeními.

Klíčová slova: kybernetická bezpečnost, kybernetický útok, malware, Metasploit, phishing, školení.

ABSTRACT

The thesis deals with the area of cyber security, focusing on the issue of user vulnerability. The theoretical part is conceived into three parts, where the introductory part is devoted to the analysis of the current state. The follow -up part summarizes the area of cyber security for understanding this industry. The third part focuses on the threats of cyber space, which we can now most often encounter.

The practical part is divided into two parts. In the first part, a cyber attack is made using an infected file according to the scenario. The whole procedure for performing the attack is accompanied by a description of the individual acts that had to be performed. In addition to outline of the attack from the attacker's point of view, it is possible to get to know the tool used in more detail. This can be used to analyze vulnerabilities for risk management purposes. The second half of the practical part is focused on the system of system security

and phishing recognition that users should be acquainted with not only a demonstrated type of attack. In the form of an attachment, training materials are processed as the output of the work, which should lead users to secure equipment.

Keywords: awareness, cyber security, cyber attack, malware, metasploit, phishing.

Tímto bych chtěl poděkovat svému vedoucímu práce panu Ing. Petru Svobodovi, Ph.D. za čas a cenné rady, které mi poskytl a díky kterým jsem mohl práci dokončit.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Zabezpečení ICT infrastruktury je pro chod moderních organizací a firem nezbytnou podmínkou. Jedná se o každodenní výzvu zainteresovaných osob udržet krok s útočníky. I zde však platí, že „řetěz je tak silný, jak silný je jeho nejslabší článek“. Ať je tato slabina způsobena nově objevenou zranitelností, neošetřením již známých zranitelností či chybným nastavením, může pro útočníka představovat onu pomyslnou skulinu, kterou se dostane do systému. V takovém případě se může celá dosud fungující bezpečnost zhroutit.

Z pohledu běžného uživatele může být problematika bezpečnosti ještě složitější. I když jsme s počítači a chytrými zařízeními v každodenním styku, mnohdy spoléháme na to, že věci, které jsou třeba pro bezpečný chod zařízení, se dějí „tak nějak samy“ či jejich důležitost bagatelizujeme. I přes úsilí bank, vlády a dalších organizací, které se v posledních několika letech snaží šířit osvětu o kybernetické bezpečnosti, jsou poměrně mezi běžnými uživateli i firmami rozšířeny názory „Nejsem nijak významný, o mě se útočníci zajímat nebudou.“, „Jsme malá firma, proč by se o nás nějaký hacker zajímal?“, „Klidně ať se mi tam někdo dostane, co si na mně vezme?“. V případě odborníků či těch, kteří měli tu smůlu a stali se obětí nějakého kybernetického útoku, není nutné vysvětlovat, že uvedená tvrzení jsou nejen mylná, ale i nebezpečná.

Zařízení užívaná bez základních bezpečnostních návyků, představují pro útočníky snazší cíle. Z hlediska firem a společností se tak na tato zařízení můžeme dívat jako na potencionální zbraně, které mohou být proti nim použity. Rozšíření povědomí o základních bezpečnostních návycích mezi běžné uživatele je tedy klíčovým faktorem pro plošné zvýšení kybernetické bezpečnosti. Koncipování školení prováděných ve firmách a organizacích způsobem, kdy by krom zaměření se na firemní prostředí byla věnována pozornost i seznámení uživatele se základními bezpečnostními návyky při používání zařízeních, v rámci jejich každodenních činností. Cílený efekt by pak pro firmy představoval krom snížení nebezpečí ze strany uživatelů nacházejících se uvnitř firemního prostředí, snížení nebezpečí v podobě ztížení získávání zařízení útočníky.

Tato diplomová práce se zabývá zpracováním případu kybernetického útoku na fiktivní společnost pro nastínění možného průniku útočníka do organizace a poskytuje konkrétní návrhy oblastí pro zavedení do školení uživatel spolu s vypracovanými školicími materiály.

VYMEZENÍ CÍLE A POUŽITÉ METODY

Práce si klade za cíl navrhnout scénář kybernetického útoku na fiktivní firmu s jeho následným provedením. Tento krok má za úkol poskytnout povědomí o způsobu, jakým se hacker může dostat pomocí phishingu do zařízení oběti, a tím i do prostředí firmy. Na základě zjištěných skutečností a zpracované teoretické části, budou navrhnuty oblasti, které by bylo vhodné zavést ve školeních kybernetické bezpečnosti ve firmách a organizacích, která mají zvýšit odolnost uživatelů vůči útočníkům. Jako konečný výstup práce pak bude zpracován materiál pro potřeby školení uživatelů v oblasti kybernetické bezpečnosti.

Hlavní cíl práce:

- Poskytnutí podkladů pro zvýšení odolnosti uživatelů vůči hrozbám v kybernetickém prostoru na základě zpracované případové studie.

Dílčí cíle potřebné pro naplnění cíle práce:

- Rešerše problematiky dané oblasti.
- Analýza současného stavu kybernetické bezpečnosti.
- Vypracování teoretického úvodu do oblasti řešené problematiky.
- Návrh scénáře a provedení útoku.
- Návrh oblastí školení kybernetické bezpečnosti pro praktické využití uživateli.
- Vypracování školicího materiálu.

Použité vědecké metody:

- **Rešerše** – zaměření rešerše v práci cílilo na dvě oblasti. První oblastí byla bezpečnostní situace, kde hlavními zdroji byly reporty společností vyvíjejících bezpečnostní software a zprávy Národního úřadu pro kybernetickou a informační bezpečnost. Druhá oblast sestávala s obecné problematiky kybernetické bezpečnosti.
- **Analýza** – Byla provedena analýza hlášených incidentů za období 2019 až 2022, na základě dat získaných z výročních zpráv Národního úřadu pro kybernetickou a informační bezpečnost.
- **Popis** – V úvodu praktické části byl popsán scénář kybernetického útoku spolu s testovacím prostředím, ve kterém byl útok simulován.

- **Simulace** – V první polovině praktické části je kontextu scénáře proveden kybernetický útok pomocí nástrojů, které mohou být k tomuto účelu využity i v reálném prostředí. Jednotlivé kroky v rámci postupu jsou detailně popsány pro utvoření celkového obrazu.
- **Modelování** – První polovina praktické části obsahuje dva diagramy. První diagram znázorňuje proces možného provedení útoku. Druhý pak představuje postup útoku, který byl proveden v rámci scénáře.
- **Indukce** – Na základě této metody, byla zvolena metoda k získání přístupu do zařízení oběti v testovacím prostředí.
- **Dedukce** – Tato metoda předpokládala nižší úroveň zabezpečení cílového systému spolu s nepozorností uživatele, která mohla být způsobena rutinním vykonáváním stejného úkonu.
- **Syntéza** – Závěrečná kapitola se věnovala sestavení témat k zařazení do obsahu školení kybernetické bezpečnosti uživatelů. Krom získání základních bezpečnostních návyků ze strany uživatelů, slouží zde představené úkoly jako opatření k zamezení útoku, který byl proveden v rámci scénáře.

I. TEORETICKÁ ČÁST

1 ÚVOD DO OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Banky, školy, státní správa, sociální interakce a navazování vztahů. Toto je jen velmi strohý výčet činností a služeb, které byly poměrně ještě nedávno spjaty primárně s fyzickým kontaktem. Dnes bychom však stěží našli některou z činností či služeb, kterou by nebylo možno vykonat v kybernetickém prostoru či by byla z kybernetického prostoru zcela vyňata. Postupným rozšiřováním o nové možnosti se stal kybernetický prostor nedílnou součástí našich životů. I kdybychom se tak snažili sebevíc, je téměř nemožné se v moderní společnosti kybernetickému prostoru vyhnout, a to i v případě, že se sami přímo na interakci s touto formou prostoru nepodílíme. Data, která jsou o nás sbírána (vědomě i nevědomě) v rámci marketingu, statistik či využíváním nejrůznějších služeb, jsou pro jejich obrovský objem ukládána v elektronické podobě. Dalším způsobem, jak můžeme zanechat stopu v kybernetickém prostoru a stát se tak jeho součástí, mohou být příspěvky našich přátel na sociálních sítích, ve kterých společně figurujeme.

1.1 Internet

Jako internet nazýváme celosvětovou síť propojených sítí, serverů a dalších zařízení, která jsou mezi sebou schopna komunikovat za účelem přenosu a výměny dat. Tato zařízení a sítě mezi sebou komunikují na základě IP adresy, která je jedním z jejich rozpoznávacích údajů v internetu a mohou být pomocí ní adresovány. Internet jako celek můžeme dále rozdělit do několika úrovní (BasuMallick, 2023). Dnes je nejběžnějším způsobem rozdělení internetu rozlišování tří jeho vrstev:

- Surface web.
- Deep web.
- Dark web.

1.1.1 Surface web

Jako surface web je označována ta část internetu, která je zobrazována pomocí běžných internetových prohlížečů. Jinými slovy je to ten internet, který známe z každodenního užívání. Při hledání v rámci surface webu stačí zadat název stránky do vyhledávače či některé ze slov obsažených ve vyhledávaném výrazu, kdy prohlížeč vyhledá stránky s tímto slovem související (Kolouch, 2016, s. 47-48).

1.1.2 Deep web

Deep web je vrstva internetu, která se nachází pod surface webem. Obsah, který se zde nachází, převyšuje ten, který je obsažen v rámci surface webu. Procházení deep webu se od toho klasického odlišuje tím, že je třeba znát přesnou adresu stránky, kterou hledáme. Oproti webům obsaženým v surface webu nejsou weby v deep webu indexovány, takže je bez přesného zadání adresy vyhledávače nezobrazí. Jedná se zejména o specifická fóra, stránky s obsahem za platební bránou, stránky pro údržbu webu, databáze atd. Pokud však přesnou adresu známe, není problém obsah zobrazit v rámci běžného prohlížeče (Belcic, Nelson, 2021).

1.1.3 Dark web

Poslední vrstvou je tzv. dark web. Na rozdíl od předešlých dvou vrstev se však dark web nachází na síti překrývající běžný internet, zvané dark net. Krom potřeby přesné adresy žádaného webu (jako tomu bylo u deep webu) je třeba disponovat i speciálním prohlížečem (případně i síťovými prvky), který je schopen se k dark netu připojit. Existuje několik takových prohlížečů, kdy nejznámějším je Tor. Tento prohlížeč je schopen krom dark webu zobrazovat i předešlé vrstvy. dark web, co do množství obsahu, představuje nejmenší část internetu. Obsah, který je zde však možné nalézt, může být mnohdy za hranou zákona. Krom samotného obsahu některých webů je zde třeba věnovat pozornost i vysokému riziku infekce, kdy se při návštěvě některého webu můžeme stát lehce obětí útočníka. Proto je třeba před potenciální návštěvou tohoto prostoru věnovat nemalé úsilí pro řádné zabezpečení nejen systému, ale i přenášených dat (Belcic, Nelson, 2021).

1.2 Kybernetická kriminalita

Vznik kybernetického prostoru sebou přinesl nespočet nových příležitostí a výhod. Avšak jak je tomu i ve světě fyzickém, „kde je světlo, je i stín“. Dnes je pro mnohé lidi online prostředí téměř nedílnou součástí jejich života. I přes tento fakt však nejsou činy kybernetické kriminality jasně definovány. Výjimku tvoří jen hlava 5 v zákoně č. 40/2009 Sb., trestní zákoník, která pojednává o trestné činnosti proti majetku. Zde jsou také uvedeny tři paragrafy, které se zaměřují na trestnou činnost proti počítačovým systémům (Česko, 2009):

- *„§ 230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací.“* (Česko, 2009, § 230).

- *„§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*“. (Česko, 2009, § 231).
- *„§ 232 Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti“.* (Česko, 2009, § 232).

Z tohoto důvodu jsou termíny vztahující se ke kybernetické kriminalitě jen „zástupnými“ názvy pro projev některého nám z fyzického světa známého trestního chování.

Hacking

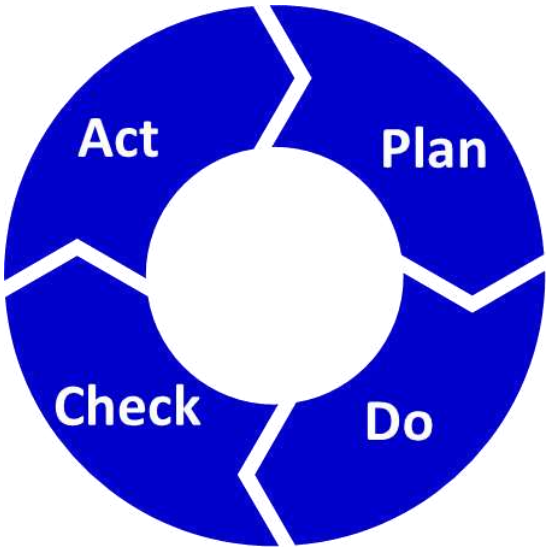
Za hackera je považován člověk, který je schopen za využití svých znalostí získat přístup do systému, sítě či organizace způsobem, který pro takovou akci není provozovatelem či výrobcem určen. Termín hacking tak zastřešuje různé techniky a postupy, kterými je možné dosažení tohoto cíle. I když je hacking společností vnímán spíše v negativním světle, spíše než na jeho provádění závisí na motivaci toho, kdo hacking prování. K základnímu rozdělení hackerů, které je založeno právě na motivaci, slouží tzv. „Klobouková metoda“ (Kolouch, 2016, s. 269-273):

- White Hats.
- Grey Hats.
- Black Hats.

Do skupiny „White Hats“ řadíme hackery, kteří svých schopností využívají k legálním činnostem. Spadá sem zejména „Red Teaming“ a penetrační testování, kdy se jedná o smluvně sjednané činnosti. Hacking je tak prováděn za účelem odhalení zranitelností a jejich následným odstraněním. Pomyslným „zlatým středem“ je skupina „Grey Hat“. Hackeři spadající do této skupiny jsou většinou motivováni dosažením prestiže v komunitě či osobního uspokojení z dosažení vytyčeného cíle. I když jejich úmyslem není uškodit, některé z prováděných činností mohou být mimo zákon. Asi nejznámější skupinou jsou však „Black Hats“. Zde řadíme hackery, kteří využívají své schopnosti ke kriminální činnosti. Mezi hlavní motivační aspekty jejich činnosti patří získání finančních prostředků, demonstrace moci či v případě hacktivismu dosažení ideologického cíle (Kolouch, 2016, s. 273).

1.3 Kybernetická bezpečnost

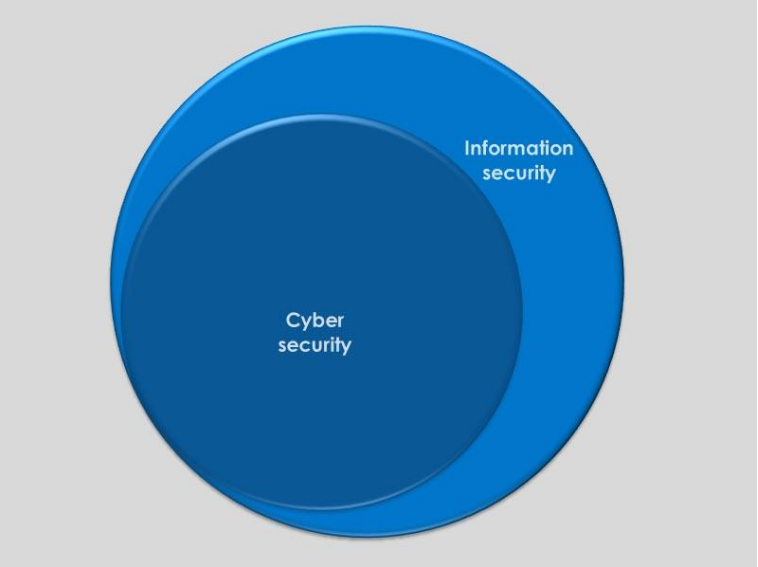
Kybernetická bezpečnost, jakožto podmnožina informační bezpečnosti, je jedním ze základních kamenů bezpečnosti ve společnostech a podnicích. Vzhledem k rychlým změnám v oblasti vývoje nových technologií a kybernetických útoků představuje udržení aktuálnosti kybernetické bezpečnosti nezbytný proces pro její zajišťování. K naplnění tohoto požadavku pomáhá docílit zakomponování Demingova cyklu do řízení všech jejich oblastí. Demingův cyklus je často označován jen zkratkou PDCA, což jsou písmena představující jednotlivé aktivity, které jsou v rámci cyklu vykonávány (plánuj, dělej, kontroluj, jednej), viz Obrázek 1 (Ondrák et al., 2013, s. 24-25).



Obrázek 1 Grafické zobrazení PDCA cyklu

(Roser, 2017)

Jak již bylo zmíněno výše, kybernetická bezpečnost je podmnožinou bezpečnosti informační, viz Obrázek 2. Hlavním rozdílem mezi informační a kybernetickou bezpečností je fakt, že informační bezpečnost se zabývá ochranou informací a dat v jakékoliv podobě, zatímco kybernetická bezpečnost se zabývá ochranou informací a dat v elektronické podobě (Kolouch et al., 2019, s. 39-40).



Obrázek 2 Informační vs. kybernetická bezpečnost
(Čermák, 2014).

I když slovo „kybernetická“ může svádět k tomu si myslet, že se jedná jen o zabezpečení dat v počítači, nemohli bychom být dále od pravdy. Abychom mohli chránit data, která jsou, byť jen v elektronické podobě, nestačí zajišťovat ochranu jen v kybernetickém světě, ale i v tom fyzickém. Obecným cílem jak kybernetické, tak i informační bezpečnosti je naplňování cílů triády CIA (Kolouch et al., 2019, s. 42-47).

1.3.1 Síťová bezpečnost

Síťová bezpečnost se zaměřuje na zabezpečení nejen perimetru sítě, ale i architektury sítě, přenosu dat v síti, rozdělení práv a přístupů v rámci sítě. Jsou zde tak uplatňována opatření pro ochranu přístupu do sítě, jako je např. zabezpečení přístupových bodů pomocí hesel a nastavení firewallu. Opatření pro monitoring narušení, jako je aplikace technologií IDS/IPS, aplikace kryptografických certifikátů pro šifrování přenášených dat atd. pro zachování třech základních požadavků v rámci triády CIA (Ondrák et al., 2013, s.161-169).

1.3.2 Aplikační bezpečnost

Aplikační bezpečnost se zaměřuje na aplikace, které jsou spuštěny v rámci ICT. Způsob zajišťování bezpečnosti aplikací bychom mohli rozdělit do dvou fází. První fází je zajištění bezpečnosti aplikace v rámci jejího vývoje. V této fázi je hlavním cílem bezpečný zdrojový kód aplikace, který zaručuje, že aplikace pracuje jen tak, jak má a neobsahuje chyby a zranitelnosti. Zanedbáním této fáze mohou být přehlédnuty chyby, které umožňují útoky, jako např. Buffer overflow, Cross-site scripting (XSS), SQL injection atd. Druhou fázi

bychom mohli pojmout jako životní cyklus aplikace od jejího nasazení až po její odinstalaci. Zde je důležité, aby byla aplikace průběžně testována, zda se u ní neobjeví zranitelnost, která by mohla být zneužita. Hlavní roli zde hraje také patch management, kdy je třeba aplikaci udržovat, pokud možno, v nejnovější verzi, aby bylo zajištěno, že jsou existující zranitelnosti odstraněny (Ondrák et al., 2013, s. 172-176).

1.3.3 Fyzická bezpečnost

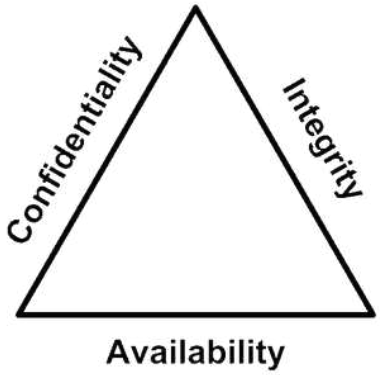
Fyzickou bezpečností v kontextu kybernetické bezpečnosti se rozumí zajištění ochrany zařízení před hrozbami, které jsou dány jejich okolím. Můžeme sem zařadit jak ochranu před poškozením v rámci havárií a mimořádných událostí, úmyslným i neúmyslným poškozením zařízení osobami, tak i ochranu před odcizením zařízení či jeho části a omezení přístupu k zařízení (Kolouch et al., 2019, s. 282-284).

1.3.4 Triáda CIA

Triáda CIA je asi nejznámější triádou, která se v kybernetické a informační bezpečnosti používá. CIA se zabývá schopností systému či organizace zajišťovat tři základní požadavky pro uchovávaná data, kterými jsou:

- Confidentiality (důvěrnost).
- Integrity (celistvost/integrita).
- Availability (dostupnost).

Jedním z hlavních úkolů při zajišťování triády CIA je dosažení rovnováhy mezi všemi jejími částmi, které se navzájem ovlivňují. Často je tak CIA zobrazována jako trojúhelník, viz Obrázek 3. Pro zajištění jednotlivých částí CIA, je vyžadováno specifických úkonů a přístupů, a to jak na procesní, tak i technické úrovni (Kolouch et al., 2019, s. 45-48).



Obrázek 3 Triáda CIA (Buntz, 2013).

Důvěrnost

Důvěrností dat je myšlen stav, kdy k datům mají přístup jen ty osoby, které jsou oprávněny s nimi jakkoliv nakládat. Tento stav se nevztahuje jen na uložená data, ale i data zpracovávaná či přepravovaná. Mezi hlavní metody pro zajištění důvěrnosti tak patří (Kolouch et al., 2019, s. 48-52):

- Kryptografické prostředky ochrany.
- Kontrola přístupů a rolí.
- Školení zainteresovaných osob.
- Klasifikace dat.

Integrita

V případě integrity dat se bavíme o datech, která jsou úplná, nepozměněná a aktuální. Pro zachování integrity dat je třeba zajistit, aby dat mohla být upravována jen osobou, která má k tomuto úkonu oprávnění. Pro naplnění tohoto požadavku jsou pak nejběžnějšími metodami (Kolouch et al., 2019, s. 52-54):

- Kryptografické prostředky.
- Hashing.
- Digitální podpisy a certifikáty.
- Kontrola přístupu a rolí.
- Samoopravné kódy.

Dostupnost

Krom zabezpečení samotné ochrany dat, kterým se zabývají důvěrnost a integrita, je taktéž třeba zajistit, aby byla data dostupná. I když se může zdát, že by zajištění dostupnosti nemusel být nijak náročný úkol, není tomu tak. Dostupnost dat či služby je udána tím, že (Hashemi-Pour, Chai, 2023):

- Je dostupná v moment potřeby.
- Je ve stanovené kvalitě.
- Tomu, kdo je k tomu oprávněn.

Dostupnost služby či dat může být krom provozních problémů či útoků omezena i samotným zabezpečením. Proto je třeba hledat optimální rozložení mezi jednotlivými body triády CIA. Nejčastější metody pro zajištění dostupnosti jsou (Hashemi-Pour, Chai, 2023):

- Redundance systému/infrastruktury.
- Zálohování dat.
- Dezpečnostní cvičení.
- Kvalitně zpracovaná bezpečností dokumentace.

1.3.5 Triáda DAD

Triáda DAD je další z triád, se kterými se ve spojení s kybernetickou bezpečností můžeme setkat. Triádu DAD bychom mohli brát jako jakýsi protipól triády CIA. Zatímco triáda CIA se zabývá spíše defenzivním způsobem ochrany, triáda DAD zaujímá ofenzivní přístup. Na rozdíl od triády CIA, která se zabývá tím, co je třeba ochránit, triáda DAD zjišťuje, jak je tyto funkce možné poškodit. Pod zkratkou DAD jsou zastoupeny tři způsoby poškození bezpečnosti dat či služby (Ydav, 2021):

- Disclosure (prozrazení).
- Alteration (pozměnění).
- Denial (odepření).

Prozrazení

Prozrazení dat je protipólem důvěrnosti v triádě CIA. Jak již bylo zmíněno výše, jedním z požadavků na důvěrnost dat je přístup jen těch osob, které jsou k tomu oprávněny. Jedná se zejména o úniky dat, a to jak úmyslně, tak i neúmyslně (Yadav, 2014).

Pozměnění

Porušení integrity dat, např. jejich pozměněním či injekcí škodlivého kódu, může představovat problém v delším časovém horizontu. Příkladem takového útoku může být úprava řídícího skriptu výrobního stroje, na základě čehož budou vyráběny špatné díly. Dalším příkladem by mohl být útok typu data poisoning. S tímto útokem se můžeme nejčastěji setkat v oblasti strojového (ML) učení a umělé inteligence (AI). Pokud útočník pozmění data v tréninkové části modelu, výsledný produkt bude mít odlišné chování. Odstranění těchto chyb je většinou zdlouhavé a nákladné (Nettles et al., 2019).

Odepření

Dostupnost dat legitimním uživatelům je stěžejní aspekt každé služby. Odepření přístupu tak může poškodit jak žadatele, tak i poskytovatele. Snad nejznámějším útokem, který cílí na tuto vlastnost systému jsou útoky DDoS. Při tomto útoku je např. stránka zahlcena požadavky od botnetu[1] útočníka. Pokud je v takovéto situaci zaslán na stránku legitimní požadavek, bude jeho vyřízení značně zpomaleno, někdy může dojít i ke „shození“ webu (Kolouch, 2016, s.295-297).

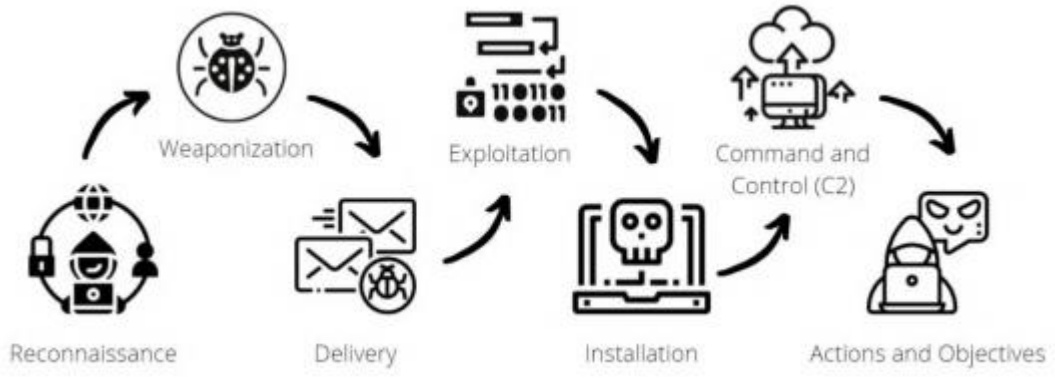
1.4 Životní cyklus kybernetického útoku

Kybernetický útok, jakožto proces, můžeme rozdělit do jednotlivých bodů, které reprezentují jednotlivé fáze útoku. Tento proces tak představuje životní cyklus kybernetického útoku. V každém bodu, resp. fázi, vykonává útočník jeden nebo více úkonů, pomocí kterých postupně formuje průběh útoku. Pro provedení jednotlivých úkonů existuje široká škála metod a technik (Sedlák et al, 2021, s. 113-114). Dnes asi nejznámějšími zdroji, které se zabývají průběhem kybernetického útoku, jsou Cyber Kill Chain, který představila společnost Lockheet Martin a ATT&CK od společnosti Mitre.

[1] Botnet – síť zařízení, které jsou ovládána hackerem. Zařízení v této síti se nazývá bot či zombie.

1.4.1 Cyber Kill Chain

Cyber Kill Chain představuje cyklus kybernetického útoku, který se skládá ze sedmi fází, viz Obrázek 4. Každá z fází je specifická činnostmi, které jsou v jejím rámci vykonávány. Fáze jsou řazeny chronologicky, avšak ne vždy jsou pro úspěch útoku uskutečněny všechny. Zde se postup odvíjí od typu útoku a cíle útočníka.



Obrázek 4 Grafické zobrazení Kill Chain (Martínez, 2022, s. 113).

Reconnaissance

Fázi reconnaissance bychom mohli přeložit jako fázi průzkumu. V této fázi podniká útočník kroky související se získáním informací o jeho cíli. K získání informací o cíli může útočník přistupovat dvojím způsobem. Prvním způsobem je získání informací pomocí sociálního inženýrství či OSINTu[2]. Zde jsou zejména sociální sítě ideálním prostředím pro sběr personálních informací o cíli. Druhý způsob se zaměřuje na technickou stránku, kdy útočník prování sken sítě či zařízení, které je mu přístupné a mohlo by posloužit jako potenciální přístupový bod. Krom skenů zde útočník využívá phishingu pro získání přístupových údajů či dalších informací, které by mohl využít např. k eskalaci práv (Diogenes, Ozkaya, 2018, s. 41-42).

Weaponization

Ve fázi, kterou bychom mohli přeložit jako vyzbrojení, si útočník připravuje na základě informací získaných v předchozích fázích nástroje, které budou využity k útoku. Většinou se však jedná o přípravu malware. Častým druhem malware je pak Remote Access Tool (RAT), který útočníkovi zajistí vzdálený přístup. Zde se setkáváme také se dvěma pojmy, kterými jsou „exploit“ a „payload“. Exploitem je myšlen kus škodlivého kódu, který cílí na zneužití zranitelnosti. Zatímco exploit má za úkol zajistit přístup do systému či sítě,

[2] Open Source Inteligence, viz kapitola 2.7.1.

payload je kusem škodlivého kódu, který způsobuje škodlivý efekt v systému (Yadav, Mallari, 2015, s. 441-442). Analogicky bychom mohli tento proces přirovnat k tankové střele. Jako exploit si představme tělo tankového granátu, který po výstřelu prorazí pancíř svého cíle. Payload je pak právě onou náloží, která po proražení pancíře detonuje a zničí cíl.

Delivery

V případě fáze doručení, je myšlen způsob, jakým útočník dopraví malware do systému či sítě. Zde se nabízí více možností, kdy příkladem může být např. phishing, stažení infikovaného souboru, připojení přenosného datového nosiče či přímá exploitace zranitelnosti síťového prvku atd. (Yadav, Mallari, 2015, s. 443).

Exploitation

Po doručení malwaru do systému je třeba, aby byl iniciován. To se mnohdy děje skrze uživatele, který daný malware obdržel. Inicializace může proběhnout formou instalace softwaru, otevřením textového souboru s povolením maker, samotným připojením USB disku do PC, návštěvou infikované webové stránky atp. Pro úspěch tohoto kroku je však kritické, aby byly splněny dvě hlavní podmínky (Yadav, Mallari, 2015, s. 443-444):

1. Systém, ve kterém dochází k iniciaci malwaru musí být zranitelný vůči exploitu, který je v malwaru obsažen.
2. Malware a jeho následná aktivita, nesmí být detekována bezpečnostními technologiemi.

Installation

Tato fáze představuje spuštění payloadu v systému, který byl exploitován v předchozí fázi. Dochází tak k instalaci backdoor, ransomware, spyware či jiného malware na zasaženém zařízení (Dholakiya, 2021).

Command and Control

Po získání přístupu do systému a provedení potřebných akcí pro „usazení se“ v systému, může být dalším krokem připojení systému k serveru, skrze který jsou od útočníka do systému zasílány příkazy k vykonání akcí. Command & Control (někdy též C2) se využívá zejména pro ovládání většího počtu zařízení, kdy asi nejznámějším využitím je botnet. V případě ovládání vícero systémů, je možné je ovládat centralizovaně. Tento krok

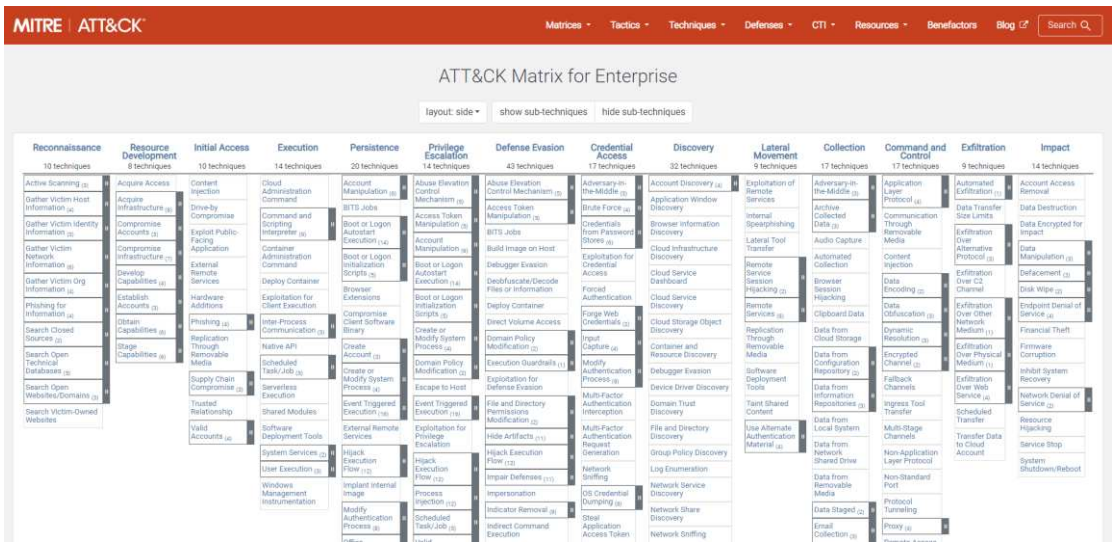
také zajišťuje útočníkovi větší bezpečnost, jelikož nekomunikuje s napadeným systémem na přímo (Lenaerts-Bergmans, 2023).

Action and Objectives

Tato fáze je poslední fází Kill Chainu. Jak již bylo zmíněno dříve, počet fází, které útočník vykoná, závisí na jeho cílech a schopnostech. Pokud se však útočník dostane až do této fáze, může vytěžovat informace ze systému a sítě v dlouhodobém měřítku, provádět akce proti dalším zařízením v síti, sbírat přístupové údaje k různým účtům, využívat zdroje systému pro těžbu kryptoměn či podnikat pomocí ovládnutých zařízení další útoky, např. DDoS (Yadav, Mallari, 2015, s. 448-449).

1.4.2 MITRE ATT&CK

Vzhledem k množství stávajících a přibývajících nových technologií je množství možností k provedení útoku takřka nekonečné. Bezpečnostní experti jsou tak denně stavěni před výzvu v udržení kroku s útočníky. I když jen stěží mohou odhadnout, s jakou novou metodou útočníci v budoucnu přijdou, mohou do jisté míry odfiltrovat alespoň ty známé. V roce 2013 představila společnost MITRE matici „Adversaries Tactics, Techniques, and Common Knowledge“, neboli zkráceně ATT&CK (Martínez, 2022, s. 117-121). Na tuto matici[3] bychom mohli pohlížet jako na databázi známých technik a postupů, které byly využity v rámci kybernetických útoků. Celá matice je uspořádána podle úkonů, které útočníci v rámci útoku vykonávají, a to od průzkumu až po možný dopad viz Obrázek 5.



Obrázek 5 Snímek MITRE ATT&CK (MITRE, 2024).

[3] Matice MITRE ATT&CK: https://attack.mitre.org/#.

Informace o tom, jak byly útoky provedeny, či jaké techniky lze využít vůči různým úrovním zabezpečení, jsou klíčovým aspektem pro pochopení chování útočníků. Toto poznání je pak základním kamenem pro budování efektivního zabezpečení.

2 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

S ohledem na proměnlivost prostředí v čase zapříčiněnou zejména socio-kulturním a technologickým vývojem je důležité si udržovat aktuální povědomí o trendech a změnách v zájmovém bezpečnostním prostředí. Pochopení zmíněných komponent, které tento prostor utváří, je základním předpokladem nejen pro uplatňování efektivních protiopatření, ale i pro predikci dalšího možného vývoje v dané oblasti.

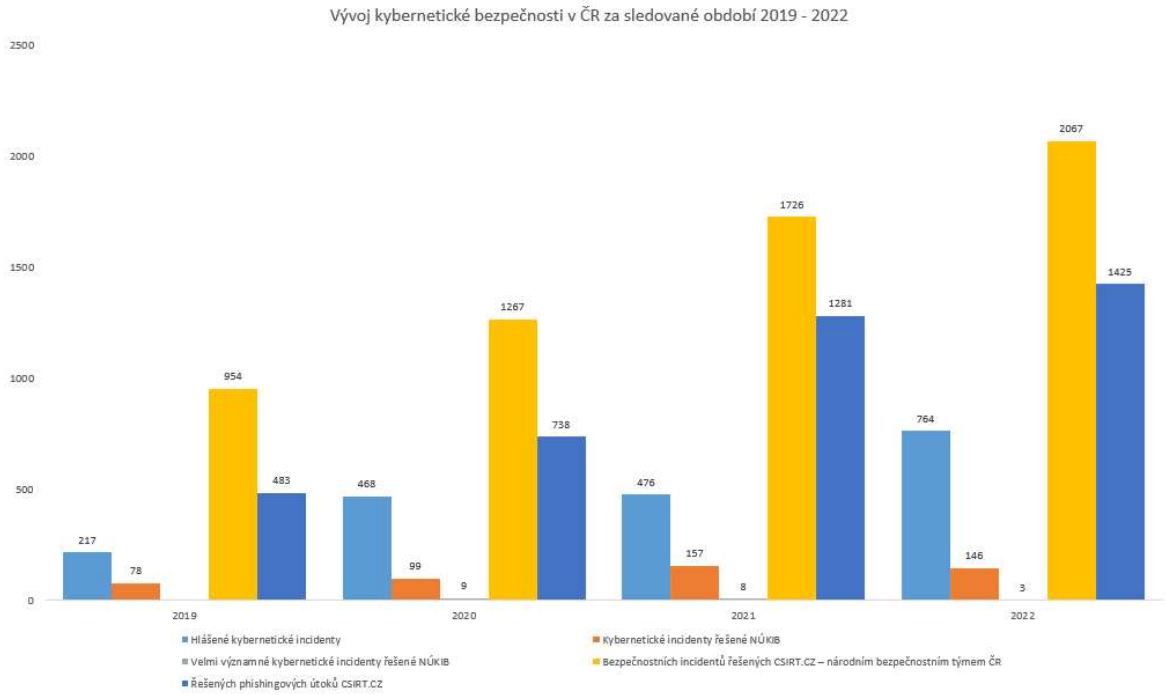
Stav kybernetické bezpečnosti v ČR bychom mohli zhodnotit na základě dvou faktorů, jejichž spojení tvoří celkový obraz o situaci. Jako první faktor bychom mohli brát reporty a zprávy organizací a institucí, které jsou v oblasti kybernetické bezpečnosti zainteresovány. Tyto reporty často obsahují konkrétní druhy malwaru, který byl zachycen produktem dané společnosti či počet řešených incidentů v daném období. V případě statistik ohledně výskytu jednotlivých druhů malwaru či forem útoků, které byly realizovány útočníky ve vymezeném období, se jedná o cenný podklad pro revizi aktuálních bezpečnostních opatření, zaměření školení uživatelů či právě predikci dalšího vývoje. Oproti tomu data udávající počet incidentů mohou být posuzována jako ukazatel atraktivity subjektu pro útočníky či jako ukazatel úrovně zabezpečení ve společnosti.

Druhý faktor pro utvoření představy o stavu kybernetické bezpečnosti v ČR je reakce státu na vývoj v dané oblasti pomocí zákonů a vyhlášek. Zákony a vyhlášky poskytují státu možnost regulace subjektů dotčeného odvětví, čímž jsou tyto subjekty nuceny splňovat podmínky uvedené v zákoně či vyhlášce. Tímto způsobem je možné určit, jakou minimální úroveň kybernetické ochrany má daný subjekt splňovat.

2.1 Přehled o stavu kybernetické bezpečnosti dle zpráv Národního úřadu pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) je ústředním správním orgánem v problematice kybernetické a informační bezpečnosti v České republice. Krom dohledu nad plněním regulačních nařízení pro povinné osoby vydává NÚKIB varování před zvýšeným bezpečnostním rizikem v rámci aktuálních hrozeb. Každoroční zpráva o stavu kybernetické bezpečnosti za dané období vydávaná úřadem poskytuje ucelené shrnutí situace v ČR. Zde jsou také uvedeny počty nahlášených a řešených incidentů v rámci

NÚKIB a CSIRT.CZ[4]. Na základě dat uvedených ve zprávách o stavu kybernetické bezpečnosti za období 2019 – 2022, viz graf Obrázek 6, můžeme sledovat vývoj v oblasti kybernetické bezpečnosti v ČR založený na počtu incidentů, které se udály v daných obdobích.



Obrázek 6 Přehled o stavu kybernetické bezpečnosti v ČR, na základě počtu incidentů v letech 2019 – 2022 (NÚKIB, 2020-2023, vlastní zpracování).

Na grafu můžeme vidět, že počty hlášených a řešených incidentů v rámci NÚKIBu a CSIRT.CZ, zaznamenal v posledních letech významný nárust. Na výrazné zvýšení počtu kybernetických incidentů (nejen v ČR) měl nezanedbatelný vliv i COVID – 19, kdy se velká část společnosti a organizací přesunula do kybernetického prostoru. I když dnes již nejsou restrikce spojené s COVIDEM – 19 uplatňovány, velká část firem, které byly touto situací donuceny pro přesun většiny činností do online prostoru, implementovaly zavedená řešení do běžného modelu jejich provozu. S přibývajícími společnostmi i jednotlivci v kybernetickém prostoru je tak pro útočníky tato oblast stále lukrativnější, a to jak po stránce finanční, tak i pro sběr informací. Meziroční nárust v jednotlivých kategoriích zastoupených v grafu je vyjádřen v tabulce, viz Tabulka 1.

[4] Computer Security Incident Response Team (CSIRT) – CSIRT.CZ je název národního CSIRT týmu České republiky, který má za úkol řešení a koordinaci v rámci reakce na kybernetické útoky.

Tabulka 1 Procentuální nárust mezi jednotlivými obdobími (NÚKIB, 2020-2023, vlastní zpracování).

Období	Hlášené kybernetické incidenty		Kybernetické incidenty řešené NÚKIB		Velmi významné kybernetické incidenty řešené NÚKIB		Bezpečnostní incidenty řešené CSIRT.CZ – národním bezpečnostním týmem ČR		Phishingové útoky řešené CSIRT.CZ	
2019	217		78		N/A		954		483	
2020	**468**	**+ 115,66 %**	**99**	**+ 26,92 %**	**9**		**1267**	**+ 32,8 %**	**738**	**+ 52,79 %**
2021	476	+ 1,70 %	157	+ 58,58 %	8	- 11,11 %	1726	+ 36,22 %	1281	+ 73,57 %
2022	**764**	**+ 60,50 %**	**146**	**- 7,01 %**	**3**	**- 62,50 %**	**2067**	**+ 19, 75 %**	**1425**	**+ 11,24 %**

Jak můžeme vidět, k poklesu došlo jen v oblastech „Kybernetické incidenty řešené NÚKIB“ za rok 2022 a „Velmi významné kybernetické incidenty řešené NÚKIB“ v roce 2021. I když došlo ke snížení v daných oblastech, celkový počet hlášených incidentů zaznamenal nárust. Krom hlášených a řešených incidentů ze strany NÚKIB či CSIRT.CZ zaznamenaly nárust taktéž pishingové útoky. Tento fakt odráží krom nárustu počtu potenciálních obětí i trend ve způsobu provedení útoku, kdy se phishing či jiné metody sociálního inženýrství těší mezi útočníky čím dál tím větší oblibě.

2.2 Vývoj dle reportu společnosti ESET

V prosinci 2023 byl vydán společností ESET report za druhou polovinu roku 2023 (ESET Threat Report H2 2023). Krom samostatných případů zkoumajících konkrétní malware uvádí tento dokument i celkový přehled ve výskytu jednotlivých druhů malware. I když ve sledovaném období došlo k poklesu výskytu útoků provedených skrze malware zaměřený na šíření skrze SMS, bankovní systémy, ransomware a ScamApp, nelze zcela říct, že by se jednalo o zlepšení celkového stavu. V témže období byl zaznamenán poměrně velký nárust spywaru a trojských koní. Konkrétně u platformy Android došlo k 89 % nárustu ve výskytu spywaru. Spyware (zejména pak v podobě infostealerů) je v posledních letech stále na vzestupu (Kopáč, 2023). Tomuto trendu významně napomáhá i fakt, že se útočníkům úspěšně daří implementovat malware do aplikací, které jsou k dostání v oficiálních obchodech, jako je např. App Store či Google Play. Vzhledem ke stále se zvyšující poptávce po datech lze předpokládat nárust i v obdobích následujících.

2.3 Zákon o kybernetické bezpečnosti

V současnosti je v České republice stále platný zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), dále jen ZoKB. Tento zákon je jeden ze základních nástrojů státu pro regulaci v oblasti kybernetické bezpečnosti. Zákon se vztahuje na osoby a orgány, které jsou vymezeny v §3 tohoto zákona

(Česko, 2014, §3, písm. a - h). Zde uvedení jsou povinni splňovat požadavky na dodržení úrovně zabezpečení dané tímto zákonem a prováděcí vyhláškou č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), dále jen vyhláška o KB.

V současnosti je však ve schvalovacím řízení nový ZoKB, ve kterém dochází k implementaci evropské směrnice NIS2. Zde dochází k sjednocení povinných osob pod jedno společné označení, a to jako „poskytovatel regulované služby“. Taktéž dochází i ke změně určení kritérií, na základě kterých bude poskytovatel regulované služby identifikován. Pro zařazení mezi poskytovatele regulované služby stačí naplnit jedno z kritérií dle §4, případně bude tak učiněno na základě rozhodnutí úřadu dle §5. Oproti současnému ZoKB dochází k nárustu, kdy z cca 300 povinných osob bude nově cca 10 000 poskytovatelů regulované služby. Toto je způsobeno zejména rozšířením odvětví, která jsou v návrhu zákona zahrnuta, velikostí společnosti jakož to jedním z kritérií a důležitostí (kritičností) poskytované služby pro společnost/stát (Česko, 2023).

3 HROZBY V KYBERNETICKÉM PROSTORU

Za kybernetický útok bychom mohli označit škodlivé jednání, které je mířeno proti aktivu či jiné osobě v kyberprostoru. Toto jednání může být provedeno jak v elektronické podobě, tak i fyzické. Dle zákona č. 181/2014 Sb. zákon o kybernetické bezpečnosti rozlišuje výsledek takového jednání na kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident. Pokud došlo ke kybernetickému útoku, který nebyl úspěšný, resp. nedošlo k poškození či narušení bezpečnosti aktiva, jedná se o kybernetickou událost. Pokud však útok nějakým způsobem omezil, poškodil či jinak narušil bezpečnost aktiva, jedná se o kybernetický bezpečnostní incident (Kolouch, 2019, s. 80-81).

Pro většinu druhů útoků využívají útočníci tzv. malware. Malware je druhem aplikace, souboru či kódu, který má škodlivý účinek na zařízení, na které je použitý. Malware bychom mohli rozdělit podle způsobu jeho šíření anebo podle jeho funkce.

3.1 Způsoby šíření malwaru

Pokud bychom se tedy zaměřili na dělení podle způsobu šíření, rozlišujeme tři základní druhy
(Langridge, 2022, s. 182-185):

- Červi.
- Viry.
- Trojské koně.

3.1.1 Červi

Jako červ se označuje malware, který se přenáší pomocí síťových paketů[5]. Červ se většinou zaměřuje na konkrétní druh/y zranitelnosti. Pokud takovou zranitelnost v systému nalezne, je schopen skrze ni proniknout do systému. Tento druh malware je také schopen se sám rozmnožovat, čímž se nejedná o jednorázovou hrozbu pro zařízení, ale pro celou síť, ve které se infikované zařízení nachází. Fakt, že je červ schopný hledat mezery v zabezpečení síťových služeb a zařízení, může být krom útoku využit při zabezpečení sítě, kdy na základě výsledků mohou být případné zranitelnosti ošetřeny (Kolouch, 2016, s. 208).

[5] Paket: jedná se o malý blok dat, pomocí kterého jsou data přenášena v síti.

3.1.2 Viry

Dalším způsobem šíření je tzv. virus, kdy se podle definice, kterou uvedl Peter Szor, jedná o „*program, který rekurzivně a explicitně kopíruje potenciálně se vyvíjející verzi sebe sama*“ (Szor, 2006, s. 39). Pro infikování zařízení virem není třeba, aby uživatel provedl nějakou dodatečnou akci. Po připojení přenosného zařízení (CD/DVD, USB, disketa atp.) k systému, otevření emailové přílohy, navštívení infikované stránky, instalaci či spuštění infikovaného softwaru, virus sám infikuje zařízení a začne se v něm samovolně šířit. Dopady infekce se pak mohou různit podle záměru, za jakým byl virus vyvinut. Můžeme se tak setkat s viry, které mohou být jen „vtípkem“ v podobě vyskakujícího textu, otevírání mechaniky CD-ROM, přehrávání různých zvuků, až po viry, které jsou schopny přeformátovat uložiště napadeného zařízení, zabránit v bootu[6] systému atp. (Aycock, 2006, s. 14-15).

3.1.3 Trojský kůň

Jako trojský kůň je označován software, který krom primární funkce, pro niž si ho uživatel pořídí, má i funkci sekundární, o které již uživatel neví. Pokud se tedy jedná např. o aplikaci pro editaci fotek, bude uživatel schopen pomocí této aplikace fotky opravdu upravovat, čímž budou naplněny jeho požadavky na danou aplikaci. Co už však uživatel nevidí je, že aplikace zároveň funguje jako spyware a odesílá získaná data. Rozšíření trojského koně je tedy zajištěno samotnými uživateli za pomoci aplikací, které jsou přímo vyvinuty jako trojský kůň, či aplikací, do který byla škodlivá funkce přidána dodatečně (může se jednat např. o Photoshop, který si uživatel nepořídí oficiální cestou, ale stáhne si jej z jiného zdroje „zdarma“) (Mukesh et al., 2016, s. 87).

Jednou z nejčastějších funkcí trojského koně, je vytvoření tzv. backdoor neboli zadních vrátek. Termín backdoor je obecně užíván pro funkci, která umožní útočníkovi přístup do zařízení. Může se tak jednat o otevření specifického portu v bráně firewall, vytvoření nového procesu zranitelné služby či uživatelského účtu atp. (Kolouch, 2016, s. 208-209).

3.2 Funkce a projevy vybraných malwarů

Vzhledem k pokroku v bezpečnostních technologiích, jsou útočníci nuceni přizpůsobovat své metody novému prostředí, tak aby byli schopni nejen proniknout do systému, ale aby při této činnosti vytěžili maximum. I proto se dnes setkáme spíše s malwarem, který

[6] Boot: jedná se o označení procesu, který probíhá při spuštění či restartu PC. Při tomto procesu je zavedeno jádro operačního systému do paměti PC.

kombinuje výše uvedené druhy. Tento malware pak označujeme podle způsobu, jakým se projeví (Aycock, 2006, s. 17-18).

3.2.1 Ransomware

Pro společnost asi jeden z nejznámějších kybernetických útoků, který je často spojen s případy, kdy se cílem staly nemocnice. Tyto případy bývají silně medializovány, což je jeden z důvodů, proč je ransomware ukotven v povědomí laické veřejnosti. Ransomware je druhem malwaru, jehož účelem je omezit funkčnost napadeného systému, omezit přístup k systému či zamezit přístupu k datům. Po získání kontroly nad systémem či daty, je uživatel vyzván k zaplacení částky pod příslibem znovuzpřístupnění systému či dat (Kolouch, 2016, s. 221-222). Podle způsobu, jakým se ransomware projevuje, jej dělíme do těchto skupin (Wickramasinghe, 2023):

- Scareware (informuje uživatele o napadení zařízení virem, na základě čehož se jej snaží přinutit k pořízení „bezpečnostního softwaru“).
- Locker ransomware (zabraňuje interakci se zařízením).
- Leakware (po zveřejnění zašifruje data na uložišti zařízení).
- Kryptografický ransomware (zašifruje data na uložišti zařízení).

V posledních letech se můžeme nejčastěji setkat právě s verzí kryptografického ransomware (Barrett, 2022). Tento fakt by se dal přisoudit postupné digitalizaci společnosti, kdy se s rostoucím objemem dat v elektronické podobě, změnil i jejich charakter. Stěží bychom dnes našli společnost či instituci, která by neukládala anebo jen nezpracovávala data v elektronické podobě. Data o uživatelích, zaměstnancích, zákaznících, ale i firemní know-how nebo rovnou celé podnikání.

WannaCry

Jedním z nejznámějších ransomware je tzv. WannaCry. Tento ransomware se objevil v květnu 2017 a masivně se rozšířil téměř po celém světě. Dle odhadů bylo zasaženo okolo 200 000 zařízení. Při napadení zařízení došlo k zašifrování dat na úložištích s následným požadavkem o výkupné, po jehož uhrazení byl zaslán dešifrovací klíč. Úhrada výkupného za zpřístupnění dat byla požadována ve virtuální měně Bitcoin. Cena za dešifrovací klíč se pohybovala mezi 300-600 dolary. Pokud oběť nezaplatila výkupné do tří dnů, cena se zvýšila. Celkové škody útoku WannaCry jsou odhadovány na 4 miliardy dolarů (Sokolov, 2022). Exploitace zařízení byla provedena pomocí MS17-010 (EternalBlue). Tento exploit

využívá zranitelnosti ve starších verzích SMBv1[7]. Pokud je exploitace úspěšná a payload je spuštěn, je krom samotného šifrování dat, zaslán packet pro objevení dalších zařízení v síti. Pokud paket nalezne zařízení, která jsou zranitelná, provede se stejný postup. Tímto způsobem je schopen se WannaCry rozšířit do všech zařízeních ve stejné síti (Secureworks, 2017).

3.2.2 Spyware

Jako spyware je označován software, jehož úkolem je sbírat data z napadeného systému. Tato data jsou následně zasílána útočníkovi. Schopnost sbírat informace v zařízení oběti je mnohdy vedlejší činností aplikace, která je prezentována jako užitečná, např. aplikace pro úpravu fotek, sledování výkonu zařízení, textový editor atd. Nejvíce se spyware šíří pomocí freeware softwaru, který si uživatel stáhne jako alternativu k placené verzi. Dalším častým způsobem, kterým se spyware dostane do systému, jsou pirátské kopie. Data, která útočník získá, mohou být použita jako zdroj informací pro účely napadení samotného systému či různých účtů a služeb. Dalším způsobem, jak je se získanými daty nakládáno, je jejich prodej (Geldenhuys, 2021, s. 15-16).

Keylogger

Asi nejznámějším zástupcem spywaru je tzv. Keylogger. Jako keylogger označujeme software či hardware, který je schopný zaznamenávat stisky jednotlivých kláves na klávesnici. Tímto způsobem může útočník získat přístupové údaje k webovým aplikacím a službám či přístupové údaje v rámci daného systému (pokud se jedná o HW keylogger, může útočník získat údaje i na úrovni BIOSu). Způsob jakým, je keylogger dopraven do zařízení, záleží na tom, zda útočník zvolil formu HW nebo SW. Pokud se jedná o HW keylogger, musí útočník získat fyzický přístup k zařízení či využít sociálního inženýrství, aby tak učinil někdo za něj. Z tohoto důvodu se ve většině případů setkáme s verzí v softwarové podobě. Ta může být v případě získání vzdáleného přístupu nainstalována do systému přímo útočníkem anebo je keylogger implementován do aplikace (Sbai et al., 2018, s. 18-20).

Infostealer

[7] Server Message Block (SMB): protokol používaný pro sdílení přístupu k souborům a komunikaci mezi uzly v síti, jako jsou např. tiskárny, sdílená uložiště atp.

V posledních letech zažívá vzestup nový druh spyware, tzv. infostealer. Infostealer, tak jako ostatní spyware, sbírá informace v prostředí napadeného systému. Oproti běžnému spywaru je však infostealer schopen jít více do hloubky, což mu umožňuje získávat i uložené přihlašovací údaje z paměti prohlížečů. Dalšími hlavními cíli pro získání dat jsou cookies, informace o samotném systému včetně informací o hardware, údaje o platebních kartách a přístupové údaje pro přihlášení se do instalovaných aplikací. Získané informace nejsou většinou posílány samostatně, ale jsou archivovány do větších celků, které se nazývají logy. Logy jsou následně odesílány k útočníkovi, který je využije buďto jako zdroj informací k proniknutí do systému či přístupu k službám, anebo jsou získaná data dále přeprodána.

Dalším bezesporu důležitým faktorem, proč je popularita infostealerů na vzestupu je fakt, že jsou poměrně snadno šiřitelné, dostupné a nevyžadují tolik znalostí pro jejich použití. Infostealery jsou většinou distribuovány jako MaaS, což je zpřístupňuje i méně zkušeným útočníku, kteří nedosahují úrovně znalostí pro vývoj vlastního malwaru. Asi nejpoužívanější způsob pro šíření infostealeru je forma trojského koně. Nejčastěji tak dochází k infekci zařízení skrze (CybelAngel, 2023):

- Cracknuté hry, aplikace a další software.
- Doplňky webových prohlížečů.
- Phishingové emaily.
- Programy pro crackování hesel.
- Software pro obnovu účtu.
- Software pro urychlení PC.
- Freeware.

Nejznámějšími zástupci jsou (Aldam, 2023):

- Racoon.
- Lumma.
- Redline.
- Vidar.

3.3 Sociální inženýrství

Existuje mnoho pohledů a definic, jak vymezit tento pojem, přičemž každý může utvořit odlišnou představu o tom, co sociální inženýrství vlastně je. Jako první příklad bych zde uvedl definici, kterou formuloval Jan Kolouch v knize CyberCrime: „*…jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli*“ (Kolouch, 2016, s. 186). Druhá definice pochází z knihy Social Engineering: The Science of Human Hacking, kde Christopher Hadnagy definuje sociální inženýrství jako „*…jakýkoli akt, ovlivňující osobu k podniknutí kroků, které mohou ale nemusí být v jejím zájmu“* (Hadnagy, 2018, s. 7). Jelikož se však tato technika v kontextu rozvoje společnosti neustále vyvíjí, nemusí být tyto definice s postupem času dostačující.

S ohledem na pokrok v bezpečnostních technologiích je pro útočníky stále těžší proniknout do systému či sítě a nároky na jejich schopnosti se tak rychle zvyšují. Tímto se stává člověk nejslabším článkem v zabezpečení. Pro spoustu útočníků se tak může stát sociální inženýrství, krom nástroje pro získávání informací a dat při přípravě útoku, i „vstupní branou“ do jinak dobře zabezpečeného systému či organizace.

3.3.1 Open source inteligence (OSINT)

OSINT je metodou, při které jsou shromažďovány informace dostupné z veřejných zdrojů. OSINT jako takový má využití ve vícero odvětvích. Příkladem může být průzkum sociálních sítí marketingovou agenturou pro vytvoření cílenější reklamy či část činnosti zpravodajských služeb. Různé techniky OSINT můžeme využít i v osobním životě, kdy pomocí např. Google dorks zefektivníme vyhledávání na internetu (Baker, 2023, s. 3-5). Pro útočníky je OSINT jednou ze základních metod, zejména pak v přípravě na cílený phishing. V takovém případě se pro ně stává internet, zvláště pak sociální sítě, rozsáhlou databází informací, které mohou být klíčové pro úspěch útoku. Zde nahrává trend dnešní společnosti, kdy „nesdílená aktivita jako by se nestala“. Takové množství sdílených událostí a aktivit, usnadňuje útočníkovi vydávání se za dotyčnou osobu. Jelikož jsou nezřídka sdíleny i informace o pracovních pozicích či různé zážitky z pracovního dne, představuje tento trend i nemalé riziko pro samotné podniky, které daného uživatele zaměstnávají.

OSINT, jak by se mohlo z výše uvedeného zdát, nespočívá jen v „brouzdání“ po internetu, ale zahrnuje i metody, které jsou více technicky zaměřeny a využívají specifické nástroje. Tímto způsobem lze odhalit chyby v nastavení webu či sítě společnosti, jako jsou např.

zveřejněné databáze, dokumenty či data, která „prosákla“ na veřejnost (Bazzell, 2023, s. 171-176).

3.3.2 Phishing

Jeden z nejrozšířenějších a nejznámějších kybernetických útoků, který je dnes častokrát skloňován ve vztahu ke kybernetické bezpečnosti. Tato technika sociálního inženýrství je zaměřena na rozesílání emailů, ve kterých se útočník snaží v oběti budit dojem důvěryhodnosti. Tyto podvodné emaily jsou často zaměřeny na krádež přístupových údajů, kdy odkaz směřuje na falešnou stránku poskytovatele služby (např. emailu či bankovnictví). Dalšími často využívanými formáty podvodných emailů je vydávání se za blízkou či oběti známou osobu (např. rodinný příslušník nebo nadřízený ze zaměstnání), emaily sloužící k šíření scamu[8] anebo pro samotné doručení malwaru (Hadnagy, 2018, s. 229–230).

V případě phishingu většinou mluvíme o hromadném šíření podvodných emailů, jehož záměrem je zasažení co největšího počtu potenciálních obětí. Existuje však vícero forem phishingu, kdy dalšími častými formami jsou spear-phishing a whaling. Spear-phishing se liší od klasického phishingu tím, že si útočník vybírá konkrétní oběť. Tou může být např. konkrétní zaměstnanec firmy, kterého vybízí útočník vydávající se za kolegu či nadřízeného, k provedení nějaké akce či získání informací (Kolouch, 2016, s. 264-265). Whaling je téměř stejný jako spear-phishing. V případě whalingu si však útočník vybírá oběti z řad vyšších pozic (např. ředitel ekonomického úseku společnosti) (Lutkevich et al., 2021).

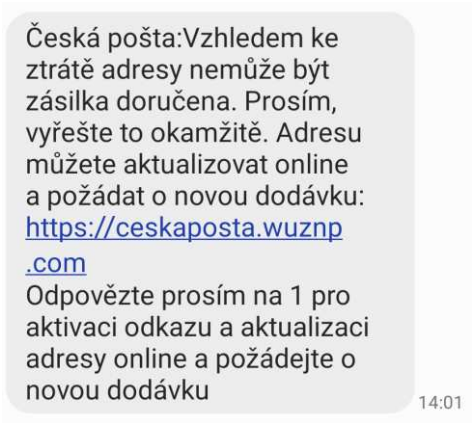
3.3.3 Vishing

Vishing je formou phishingu, kdy je ke kontaktování oběti využito telefonu. Tato technika sociálního inženýrství klade na útočníka vyšší nároky z hlediska přípravy a samotného provedení. Jelikož útočník komunikuje přímo s obětí, mohly by nedostatky vědomostí ohledně tématu konverzace či nervozita vzbudit podezření (Kolouch, 2016, s. 265). I přes tento fakt je vishing poměrně běžný. Útočníci se nejčastěji vydávají za podporu z banky či policii, která oběť informuje o neobvyklém pohybu na jejím účtu. Pod záminkou ochrany jsou od oběti požadovány přístupové údaje k účtu, či rovnou převod peněz na „bezpečný“ účet. Dalším obvyklým tématem jsou investice, kdy se útočník snaží přimět oběť pod záminkou investice k převodu peněz na jeho účet.

[8] Scam – jedná se o podvod, jehož účelem je získání finančních prostředků oběti.

3.3.4 Smishing

Smishing tak jako vishing je formou phishingu, kdy se ke kontaktování oběti využívá SMS zpráv. Oproti předešlým dvěma formám je také méně využívaný (Hadnagy, 2018, s. 240). Útočníci se v případě smishingu často zaměřují na doručovací společností či poštovní služby. I když se jedná o méně používanou formu, v období Vánoc vzhledem ke zvýšeným nákupům nabírá na intenzitě, viz Obrázek 7.



Obrázek 7. Podvodná urgence od České pošty (vlastní).

3.3.5 Quishing

Quishing patří mezi novější způsoby phishingu, přičemž v rámci jeho provedení je využit Quick Response Code neboli QR kód. QR kód je ve světě zejména mobilních zařízení velmi rozšířenou a pro svoji funkčnost i oblíbenou technologií. QR kód je forma 2D obrazce, který stejně jako čárový kód je schopen reprezentovat data. QR kód je však svou strukturou schopen pojmout dat více. Data a informace, které jsou QR kódem prezentovány, mohou obsahovat různou grafiku, dokumenty, odkazy či další informace a úkony. Dnes jsou QR kódy široce rozšířeny, přičemž při adaptaci do společnosti významně napomohla situace v rámci COVID – 19 a fakt, že pro jejich čtení stačí smartphone. Krom zobrazování psané formy sdělení informací jsou QR kódy hojně využívány pro provádění bankovních plateb. Pro útočníky tak představuje QR kód ideální prostředek pro podvodné platby či ukrytí odkazu směřujícího na infikovaný web (Irei, 2023).

3.4 Advanced Persistent Threat (APT)

Advanced Persistent Treat neboli Pokročilá a trvalá hrozba. Na tuto problematiku by se dalo pohlížet dvojím způsobem. Prvním APT jako samotný kybernetický útok, druhým je APT

jako označení konkrétní hackerské skupiny či státní složky a jimi podporované skupiny[9]. APT jako samostatný kybernetický útok znamená dlouhotrvající sofistikovaný útok proti organizaci či státu. Takový útok je pak zpravidla prováděn hackerskými skupinami či státními aktéry, jelikož pro provedení takového útoku je vyžadováno velké množství zdrojů, a to jak finančních, tak i technických a vědomostních (Kolouch, 2016, s. 320-322). Právě aktéři APT jsou hlavním dodavatelem nových zranitelností a exploitů, které se po použití stávají známými metodami i pro širší hackerskou a bezpečnostní komunitu, viz MITRE ATT&CK.

3.5 Hacking jako business

S rostoucí digitalizací společnosti, se stal kybernetický prostor téměř nedílnou součástí každodenního života lidí po celém světě. Pro mnohé jednotlivce a organizace tak vznikla nová platforma, na které lze vybudovat či jen rozšířit své podnikání. Z hlediska státních institucí vznikla nová cesta, jak poskytovat služby občanům. S příchodem cloudu se tempo digitalizace a možnosti rozvoje v digitálním světě ještě zvýšily. Nejčastěji nabízenými modely cloud computingu jsou pak:

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service (SaaS).
- Network as a Service (NaaS).

Tohle všechno sebou přineslo i velké množství finančních prostředků, které se v kybernetickém světě pohybují. Útočníci jsou tak motivování nejen prestiží v komunitě či ideologickými cíli, ale i vysokými finančními zisky. Krom financí získaných ze samotného útoku, např. výkupným za ransomware či prodejem ukradených dat, se rozvinula i činnost známá jako Cybercrime as a Service neboli (CaaS). V případě CaaS se nejedná jen o provedení samotného útoku, ale i o prodej některé komponenty či konkrétního řešení, kterou lze k útoku využít. Můžeme se tak například setkat se službami jako jsou (Nobles et al., 2023, s. 105-107):

- Ransomware as a Service (RaaS).

[9] Např. APT29, což je označení pro ruskou hackerskou skupinu „Cozy Bear“.

- Malware as a Service (MaaS).
- DoS/DDoS as a Service (DaaS).
- Access as a Service (AaaS).
- Phishing as a Service (PaaS).

Díky možnosti, dostupnosti a konkurenčnímu prostředí, ve kterém je možné zakoupení některé ze služeb CaaS, značně přispělo k nárustu kybernetických útoků po celém světě. A to jak z důvodu rychlosti při přípravě útoku, tak i umožnění méně zkušeným útočníkům provádět sofistikovanější útoky, kterých by dříve nebyli schopni.

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Kybernetická bezpečnost se stává stále více nepostradatelnou komponentou při zajišťování bezpečnosti v organizacích a státech, ale také v soukromém životě. Míra provázanosti fyzického světa s tím digitálním roste každým rokem. Zatímco ze strany organizací se kybernetické pozornosti začíná dostávat potřebné pozornosti, v případě běžných uživatelů může být tato potřeba přehlížena. Avšak, ať už se jedná o vědomé bagatelizování této potřeby, či její přehlížení v důsledku nedostatečného povědomí o dané problematice, představuje tento stav jak pro firmu, tak i pro stát zranitelnost, která je útočníky vysoce exponována.

Proto je třeba stále hledat nové možnosti a formy, kterými lze rozšířit povědomí o důležitosti této oblasti bezpečnosti mezi uživateli. Ukotvení základních bezpečnostních návyků v uživatelích při jejich pohybu v online světě či každodenního užívání ICT zařízeních, zvýší odolnost proti hrozbám v kybernetickém prostoru nejen u samotných uživatelů, ale i státu a firmách, kde pracují.

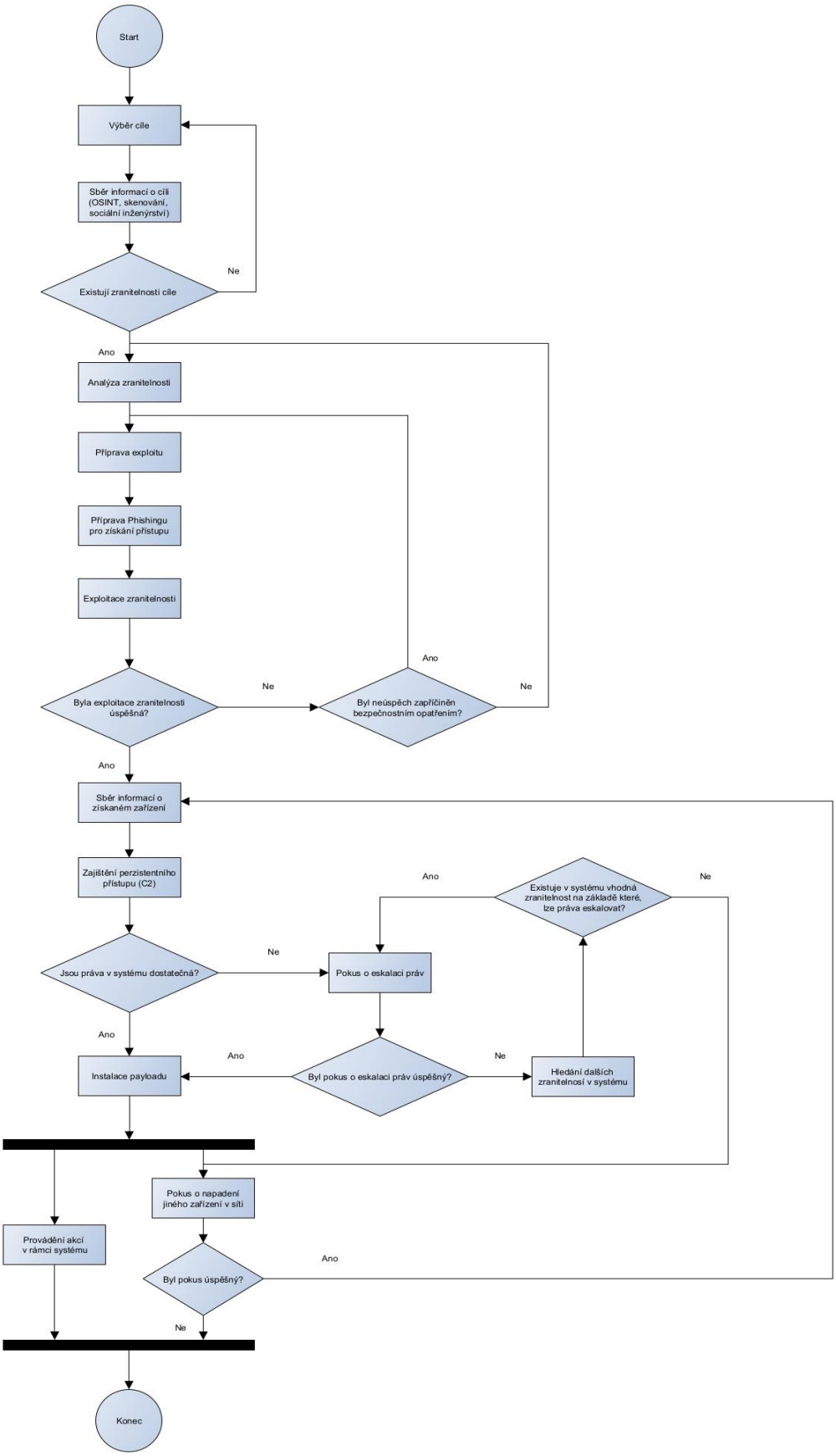
II. PRAKTICKÁ ČÁST

4 PŘÍPADOVÁ STUDIE PHISHINGOVÉHO ÚTOKU

V této kapitole se budu zabývat provedením možného postupu při získání přístupu do jiného počítače. Vzhledem ke komplexitě problematiky kybernetických útoků, která skýtá nepřeberné množství způsobů jejich provedení, zde uvádím grafické znázornění možného průběhu pomocí diagramu, zejména pro lepší orientaci v nadcházejících kapitolách, viz Obrázek 8.

Scénář útoku se bude odehrávat ve fiktivní firmě, ve které se nachází počítač s operačním systémem Windows 8.1, jehož zabezpečení obsahuje několik bezpečnostních mezer. Starší systémy jsou mezi uživateli poměrně časté, jelikož nové operační systémy vyžadují vyšší nároky na hardware, což by mohlo znamenat pořízení nového zařízení. Taktéž uživatel sám nemusí cítit potřebu přecházet ze systému na který je již zvyklý na nový, u kterého by si musel zvykat na nové prostředí. Pro provedení útoku jsem zvolil Kali Linux. Jelikož se jedná o distribuci předurčenou k penetračním testům, obsahuje tak již předinstalované nástroje vhodné pro tuto demonstraci. I když se z hlediska technické úrovně provedení nejedná o zvláště sofistikovaný pokus a před moderním zabezpečením by neobstál, pro účely demonstrace možného postupu útočníka je však dostačující.

Podklady získané touto demonstrací či demonstrace samotná v rámci školení, jsou prvkem, který může upoutat pozornost. Probuzení zájmu či jen zvědavosti v rámci školení napomáhá v překonání počátečního nezájmu či odporu k danému tématu ze strany posluchačů. S tímto problémem je možné se setkat snad v každé firmě, kde školení zaměstnanců probíhají, zejména pak v případě starších či méně technicky zdatných zaměstnanců. Pokud školitel dokáže překonat tyto překážky, je zde předpoklad ke zvýšení efektivnosti těchto školení, a tím i zvýšení bezpečnosti ve společnosti.



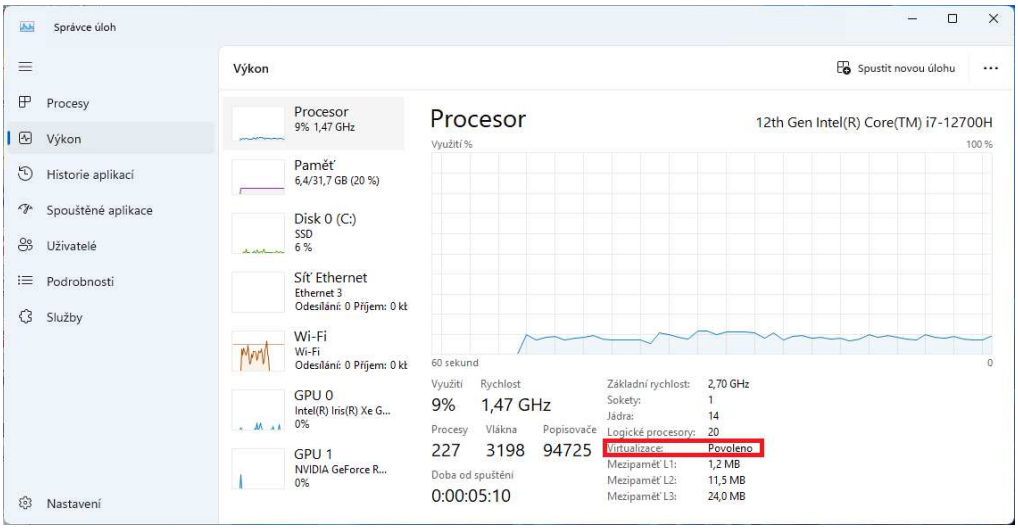
Obrázek 8 Diagram možného postupu v rámci kybernetického útoku (vlastní zpracování v softwaru yEd).

4.1 Testovací prostředí

V této části bych chtěl představit blíže některé z nástrojů, které jsem využil při simulaci útoku. Konkrétně se jedná o VirtualBox, ve kterém jsem nastavil virtuální prostředí. Dále Kali Linux, který posloužil jako hlavní operační systém. Pro většinu úkonů v rámci simulace jsem pak využil nástroje Metasploit, který je již v základu součástí Kali Linuxu.

4.1.1 Virtuální prostředí

Virtualizace umožňuje provozovat vícero operačních systémů na jednom počítači či serveru. Krom využití v produkčním prostředí nebo cloudu je virtualizace vhodná pro vytvoření testovacího prostředí či sanboxu. Virtuální systém využívá zdroje PC, na kterém běží. Jinak se jedná o systém, který je od systému, ve kterém běží, izolován. Pro vytvoření virtuálního stroje (dále jen VM), je nutné splnit několik podmínek. Prvním předpokladem pro možnost vytvoření VM je procesor, který virtualizaci umožňuje, což by však v dnešní době neměl být problém. To, jestli náš procesor podporuje virtualizaci, nebo zda je možnost virtualizace povolena, můžeme zjistit jednoduše ve správci úloh, viz Obrázek 9.

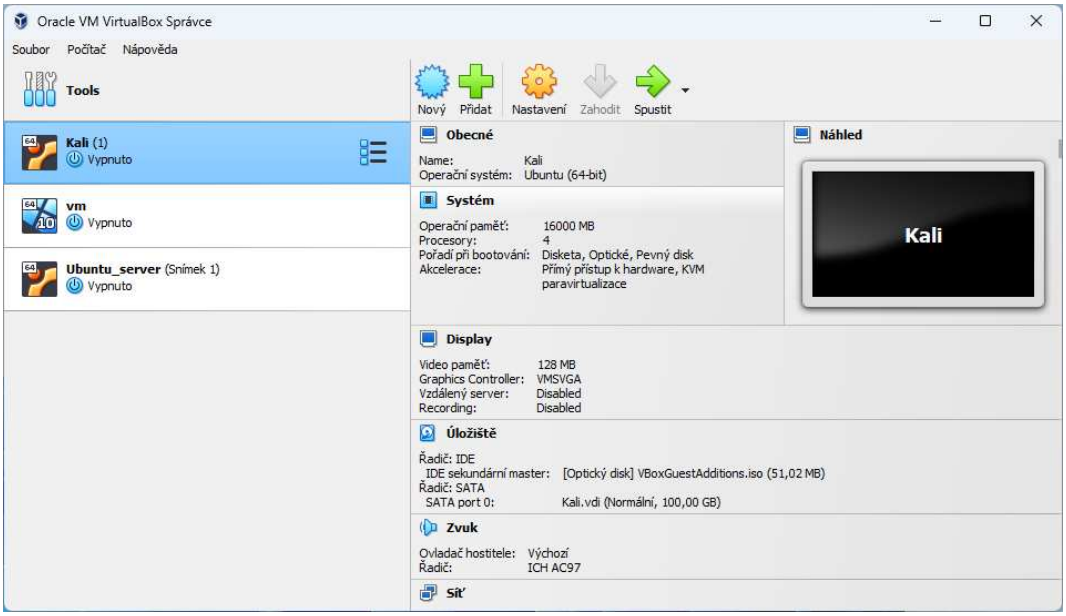


Obrázek 9 Kontrola povolení virtualizace (vlastní).

Pokud virtualizace povolena není, lze ji zapnout v BIOSu počítače. Pro přístup do BIOSu počítače je třeba při bootu systému zmáčknout klávesu, která je definována výrobcem, v závislosti na výrobci se můžou klávesy lišit. Většinou se však jedná o některou z kláves F1– F12 nebo klávesu DEL. Po zpřístupnění BIOSu hledáme řádky s názvy jako jsou např. VT-x, Virtualization Technology, AMD-V atd. Zde pak změníme status služby z „Disabled“ na „Enabled“. Nejčastěji se toto nastavení nachází v oddílu „Advanced“ či „Security“, viz Obrázek 10.

Obrázek 10 BIOS a povolení virtualizace (Vlastní).

Pokud se chystáme ve VM využívat zdroje hardwaru jako je grafická karta, síťová či zvuková karta atd., je třeba zapnout i VT-d, čímž umožníme VM přímý přístup k hardwaru. Pokud však VT-d nepotřebujeme, je lepší jej pro zvýšení bezpečnosti vypnout. Pokud je virtualizace povolena, můžeme rovnou přejít k instalaci softwaru, pomocí kterého budou VM vytvořeny. Virtuální prostředí pro účely této práce je vytvořeno pomocí nástroje VirtualBox od společnosti Oracle, viz Obrázek 11. Instalační soubor VirtualBoxu lze volně stáhnout z oficiálních stránek https://www.virtualbox.org. Vytvoření virtuálního prostředí ve VirtualBoxu je poměrně jednoduché, kdy pro někoho může být hlavní výhodou ovládání přes GUI.



Obrázek 11 Správce VirtualBox (vlastní).

Pro vytvoření nového virtuálního stroje budeme potřebovat ISO soubor s operačním systémem. Výběrem záložky „Nový“ otevřeme okno, ve kterém vybereme zamýšlený systém pro VM, nastavíme velikost přidělené operační paměti, vytvoříme virtuální disk a zvolíme ISO soubor obsahující operační systém. Nastavení jednotlivých parametrů záleží na zamýšleném účelu. Neměli bychom však nastavovat nižší parametry, než jsou minimální požadavky definované výrobcem. Pokud bychom potřebovali některé z parametrů upravit, je možné další nastavení provádět pod záložkou „nastavení“. Zde také nalezneme nastavení sítě. Pro zvolení správného nastavení sítě doporučuji postupovat podle tabulky 6.1 viz, Obrázek 12 Natavení sítě ve VirtualBox (Oracle, 2024).

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	–	–
Internal	–	–	+	–	–
Bridged	+	+	+	+	+
NAT	+	Port forward	–	+	Port forward
NATservice	+	Port forward	+	+	Port forward

Obrázek 12 Natavení sítě ve VirtualBox (Oracle, 2024).

4.1.2 Kali Linux

Kali Linux (viz Obrázek 13) byl vyvinut s cílem poskytnutí prostředí pro bezpečnostní experty zabývající se zejména penetračním testováním a forenzní analýzou. Jedná se o distribuci založenou na Debianu, o jejíž správu se stará společnost Offensive Security, která krom udržování aktualizací nadále pokračuje ve vývoji. Po instalaci jsou tak již

připraveny nástroje, pomocí kterých je uživatel schopen provádět např. skenování sítě, analýzu škodlivého kódu, či nástroje pro sociální inženýrství, prolamování hesel atp. Další nástroje jsou také vyvíjeny širokou komunitou, kdy většina i původních nástrojů jsou na bázi open-source. Samotný Kali Linux je pak volně k dostání na oficiálních stránkách https://www.kali.org.

Obrázek 13 Pracovní plocha Kali Linuxu (vlastní).

4.1.3 Metasploit

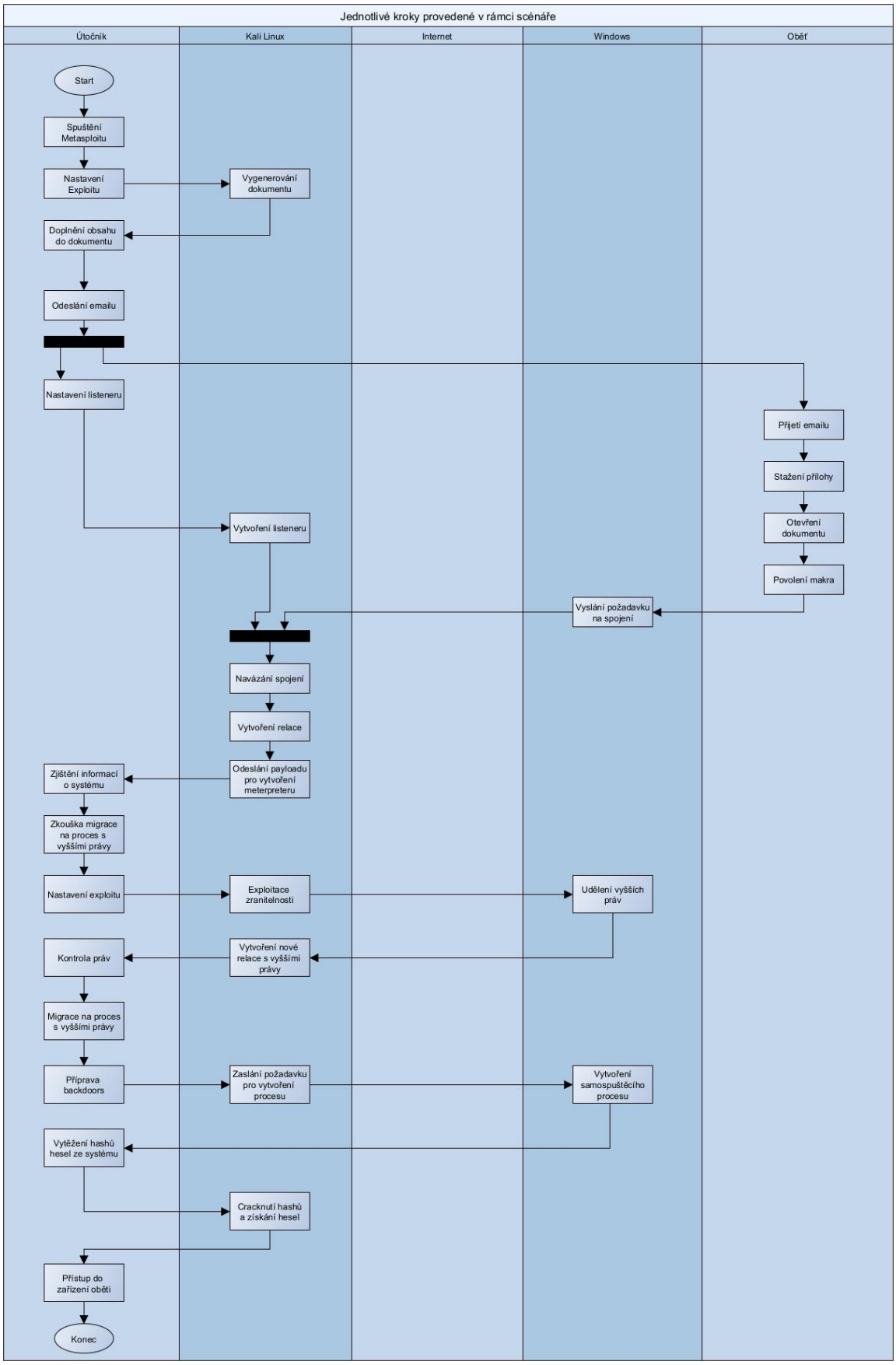
Jako hlavní nástroj pro provedení názorného útoku jsem zvolil Metasploit. Metasploit je nástroj, určený primárně k penetračnímu testování. Dnes je spravován společností Rapid7 a je dostupný ve dvou provedeních. Prvním je Metasploit-framework, který je jakožto open-source zdarma. Druhým provedením je Metasploit Pro, kde se jedná o placenou verzi Metasploitu, která přináší oproti open-source verzi značné výhody, např. není tak známá bezpečnostním softwarům. Pro účely práce je však použita open-source verze, jelikož je dostupná pro každého. Tato verze však neposkytuje takové možnosti jako ta placená a vzhledem k její rozšířenosti jsou šablony, kterými disponuje, dobře známy bezpečnostním softwarům. Zatímco pro začátečníka v oblasti penetračního testování se může jednat o podstatnou překážku, pokročilí uživatelé jsou tento nedostatek schopni vykompenzovat možností úprav jednotlivých šablon, které si mohou přizpůsobit dle své potřeby. Metasploit-framework se skládá z pěti základních modulů (Buckbee, 2022):

- Exploity (kód, který zneužívá zranitelnosti).
- Payloady (kód, který provádí akci na cílovém zařízení).
- Auxiliary (používají se jako skenery, fuzzery či generátory pro DoS).

- Post-Exploitation (slouží pro sběr informací v napadeném systému).
- NOP generátor (generátory náhodných bitů pro obcházení IDS/IPS).

4.2 Scénář

Fiktivní firma Obrábění, s. r. o. se zabývá výrobou spojovacího materiálu. Jedná se o mladou firmu s patnácti zaměstnanci. Z důvodu zakoupení nového obráběcího stroje se firma rozhodla najmout dalšího pracovníka, který by byl schopný s tímto strojem pracovat. Paní Zdena, které se stará ve firmě o účetnictví a personalistiku, proto umístila na web prácerychle.cz inzerát na pozici „CNC seřizovač“. Tohoto se rozhodl využít útočník, jakožto možnosti získání přístupu do firemního prostředí. Útočník vypracoval životopis, do kterého nahrál makro pro navázání spojení s cílovým systémem. Po otevření životopisu, získal útočník přístup do počítače paní Zdeny. Zde eskaloval práva, aby mohl vykonávat úkony s administrátorským oprávněním, které mu krom jiného umožnily vytvořit backdoors pro opětovný přístup do počítače. Tímto získal útočník výchozí bod pro provádění dalších akcí. Krom krádeže dat z infikovaného počítače, tak mohl prodat samotný přístup do firmy, skenovat vnitřní síť podniku a útočit na další zařízení, či využít ransomware atd. Pro lepší orientaci v rámci provedení modelového útoku slouží zpracovaný diagram, viz Obrázek 14.



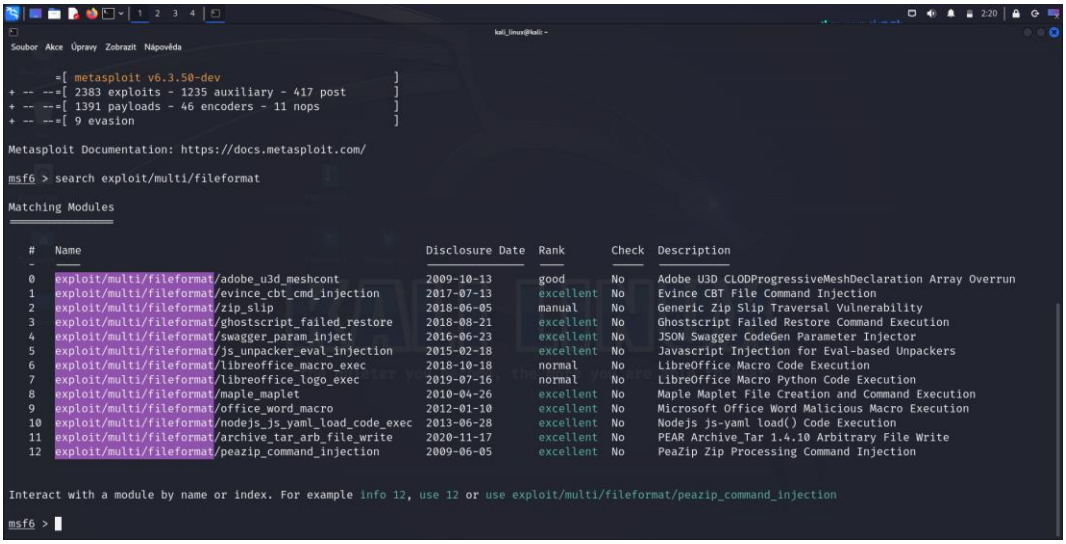
Obrázek 14 Grafické zobrazení postupu v rámci scénáře (vlastní zpracování v yEd).

4.3 Příprava dokumentu

Po dokončení instalace systému, aktualizaci a případným dalším nastavením v rámci individuálních preferencí můžeme začít připravovat dokument, pomocí kterého získáme přístup do systému zařízení, ve kterém bude soubor otevřen. V terminálu pomocí příkazu „msfconsole“ spustíme nástroj Metasploit-framework, viz Obrázek 15.

Obrázek 15 Metasploit CLI (vlastní zpracování v Metasploit Framework).

Metasploit-framework má vlastní konzoli. Pomocí příkazu „help“ si můžeme zobrazit přehled příkazů, které slouží k interakci s konzolí. Jak bylo již zmíněno výše, útočník využil k přístupu do organizace infikovaný soubor. Metasploit-framework disponuje exploity, které jsou zaměřeny na textové soubory. Pomocí příkazu „search exploit/multi/fileformat/“ zobrazíme nabídku dostupných exploitů, viz Obrázek 16. Není třeba psát celý název, Metasploit vyhledá všechny položky, které souvisí s momentální podobou zápisu.



Obrázek 16 vyhledání exploitu (vlastní zpracování v Metasploit Framework).

Nad seznamem nalezených modulů se nachází hlavička, která nám poskytuje první informace o daném modulu:

- Číslo v pořadí výpisu.
- Name/jméno.
- Disclosure Date/datum vytvoření modulu.
- Rank/hodnocení.
- Check/ověření.
- Description/popis.

Číslo, které udává pořadí modulu v celkovém výpisu, lze použít místo celého zápisu jména modulu. Jméno modulu je vlastně cesta, která vede k souboru tvořícího modul. Pokud je již uživatel seznámen s některými moduly, může tak rovnou psát jméno modulu, aniž by před tím použil vyhledávání skrze příkaz „search“. Disclosure Date uvádí, kdy byla zveřejněna zranitelnost, na kterou exploit cílí anebo, kdy byl modul do Metasploitu přidán. Krom zamýšlené funkce modulu je asi nejdůležitějším ukazatelem „Rank“. Rank je rozdělen do několika úrovní, každá úroveň udává spolehlivost/náročnost využití modulu. Pokud je hodnocen např. exploit hodnocen jako „manual“, je docela pravděpodobné, že jeho použití vůči systému bude mít nezamýšlený účinek (exploitace se nezdaří, cílový systém se restartuje atp.). Sloupeček „Check“ obsahuje jen dvě hodnoty „yes“ a „no“. Tyto hodnoty informují uživatele, zda je pro daný modul dostupný příkaz „check“, který má za úkol prověřit, zda je cíl vůči zvolenému modulu zranitelný, aniž bychom použily samotný modul.

Poslední kolonkou „Description“ je popis modulu, kde je v 1-2 větách uvedena funkce modulu. Nalezený exploit zadáme pomocí příkazu „use exploit/multi/fileformat/office_word_macro“, anebo „use 9“. Další informace o zvoleném exploitu můžeme získat zadáním příkazu „info“. Pokud bychom chtěli detailnější výpis, můžeme použít příkaz „info -d“, kdy nám Metasploit vypíše informace do webového prohlížeče.

4.3.1 Nastavení modulu

Po zvolení preferovaného exploitu je třeba nastavit některé z jeho parametrů. Pro zobrazení nastavení slouží příkaz „show options“, viz Obrázek 17. Parametry, které je třeba nastavit, se mohou u každého modulu lišit v závislosti na jeho charakteristice. Pokud bychom chtěli zjistit, které z parametrů jsou pro běh modulu nezbytné, můžeme je vypsat do konzole pomocí příkazu „show missing“. Parametry, se kterými se setkáme snad v každém modulu jsou LHOST/RHOST[10] a LPORT/RPORT[11].

Obrázek 17 Nastavení modulu (vlastní zpracování v Metasploit Framework).

Pokud bychom chtěli zobrazit pokročilá nastavení pomocí kterých můžeme blíže specifikovat vlastnosti modulu, učiníme tak pomocí příkazu „show advanced“. V případě, že bychom chtěli upravit samotný kód modulu, můžeme jej otevřít v editoru Vim pomocí příkazu „edit“. V rámci zvoleného exploitu jsou povinnými parametry právě LHOST a LPORT. Funkcí daného exploitu je vytvoření textového dokumentu ve formátu „.docm“. Jedná se o dokument Microsoft office, který obsahuje makro pro navázání reverzního shellu.

[10] RHOST – Remote Host/Vzdálený host, LHOST – Local Host/Lokální host
[11] RPORT – Remote Port /Vzdálená port, LPORT – Local Port/Lokální port

4.3.2 Vygenerování souboru se škodlivým kódem

Reverzní shell[12] oproti bind shellu není navázán ve směru „útočník → oběť“, ale „oběť → útočník“. Bind shell je využíván zejména v případě exploitace zranitelnosti služby vystavené „do internetu“ a může být zastaven skrze firewall. Reverzní shell využívá výhody, že síťový provoz, který směřuje ven ze sítě, zpravidla filtrován není. Musí být však iniciován obětí.

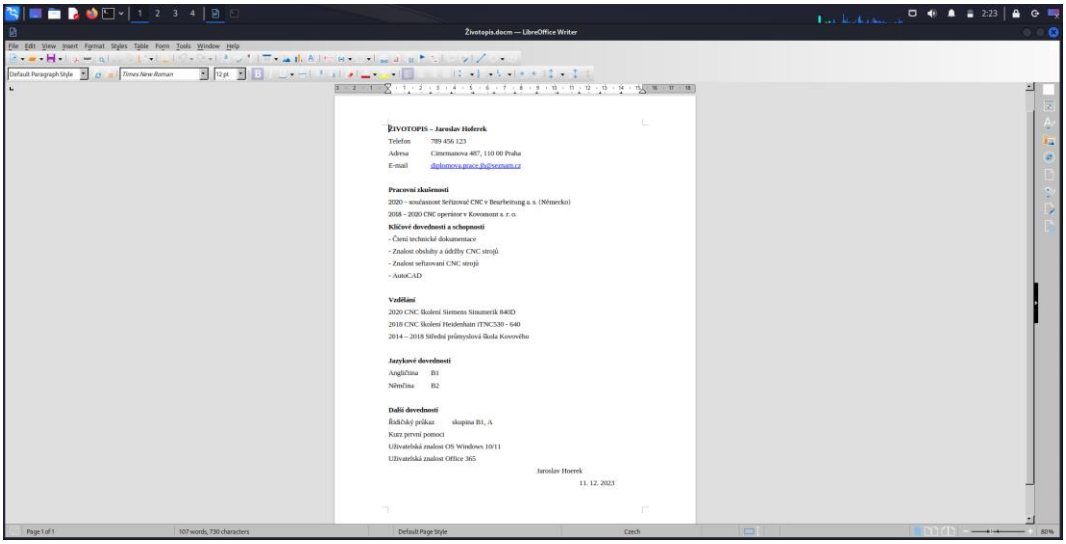
Nastavení jednotlivých parametru provádíme pomocí příkazu „set <parametr> <hodnota/stav>“. Adresu pro parametr LHOST nastavíme podle toho, zda chceme komunikovat se zařízením oběti napřímo, či zvolíme formu C2 serveru. Z důvodu, že celá simulace probíhá v rámci LAN, uvedeme lokální adresu Kali Linuxu. Lokální adresu si můžeme zobrazit pomocí příkazu „ifconfig“. Síťový port (LPORT), na který se bude zařízení oběti připojovat, zvolíme dle vlastního uvážení. Je však nutné, aby byl tento port povolen ve firewallu, jinak by bylo spojení zamítnuto. Po dokončení nastavení exploitu, jej spustíme pomocí příkazu „exploit“, čímž bude vygenerován dokument obsahující makro, viz Obrázek 18. Po dokončení generování, je v posledním řádku zobrazena cesta k souboru.

Obrázek 18 Vygenerování škodlivého souboru (vlastní zpracování v Metasploit Framework).

Jak bylo uvedeno ve scénáři, útočník se rozhodl získat přístup do organizace pomocí infikovaného souboru s životopisem, kterým odpovídá na pracovní nabídku. Jelikož firma očekává, že bude dostávat emaily s životopisy v rámci odpovědí na inzerát, může být tato cesta ideální volbou. V jiném případě by náhodný email s přílohou či odkazem mohl snadněji vzbudit podezření. Pro vytvoření infikovaného dokumentu je do něj třeba napsat

[12] Shell: jedná se o základní textové rozhraní, kterým je schopný uživatel komunikovat s operačním systémem. Příkladem mohou být u Windows Powershell a cmd, v případě Linuxu terminál.

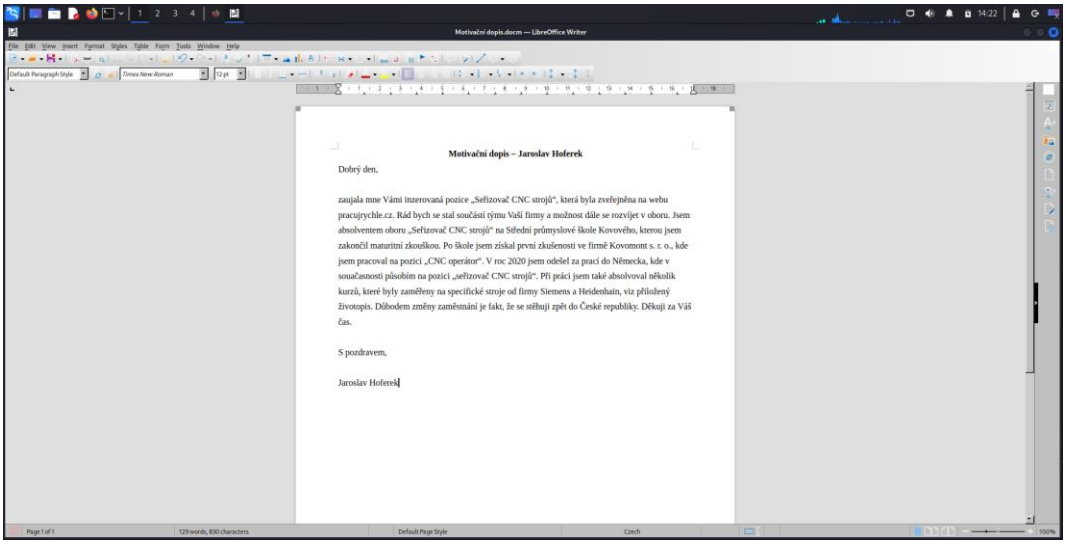
životopis, který odpovídá inzerované pozici, viz Obrázek 19. Pro tento účel můžeme použít např. LibreOffice, který je jakož to open-source software k dostání zdarma na oficiální adrese https://cs.libreoffice.org.



Obrázek 19 Životopis obsažený ve škodlivém souboru (vlastní).

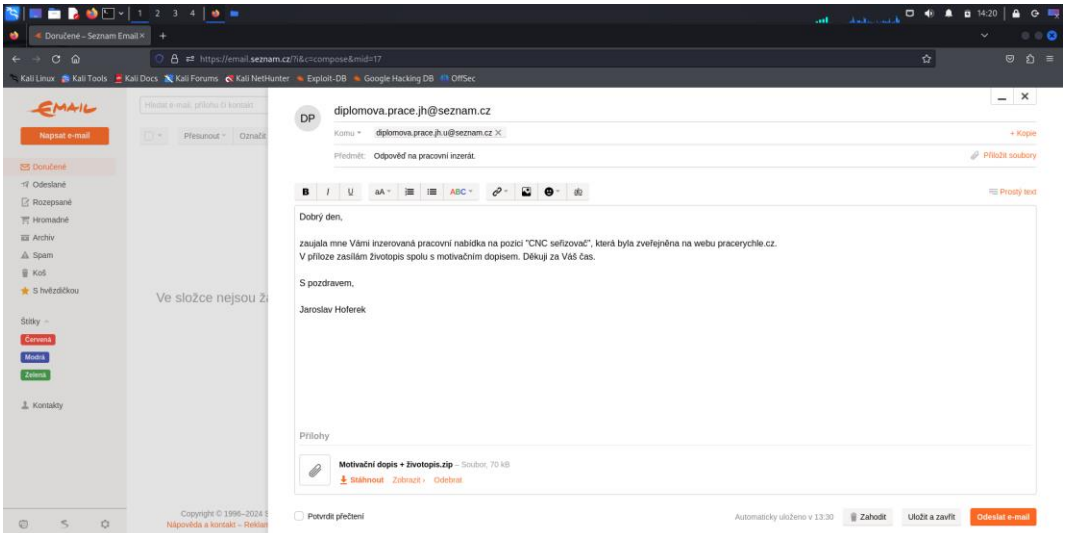
4.4 Získání přístupu

Pro získání přístupu je třeba, aby bylo splněno několik podmínek. První podmínkou je, aby se dokument dostal k oběti. Druhou podmínkou je přimět oběť, aby otevřela infikovaný soubor a povolila makra. Třetí podmínka závisí na existenci zranitelnosti vůči danému exploitu. Čtvrtá podmínka se vztahuje k antivirovému softwaru, který nesmí detekovat škodlivý kód. Pro splnění požadavků v rámci dokumentů pro ucházení se o dané místo, jsem vytvořil ještě motivační dopis, který však již škodlivý kód neobsahuje, viz Obrázek 20. Oba dokumenty budou zaslány emailem na adresu, která byla uvedena v inzerátu.



Obrázek 20 Motivační dopis (vlastní).

Po založení emailové adresy a vyplnění hlavičky emailu spolu se zprávou pro příjemce je třeba vložit do emailu i vytvořené dokumenty. Zde se však můžeme setkat s chybou při pokusu o načtení dokumentu do přílohy, jelikož emailové schránky mohou označit dokument za škodlivý. V tomto konkrétním případě byl problém vyřešen zabalením obou dokumentů do archivu „zip“, viz Obrázek 21.

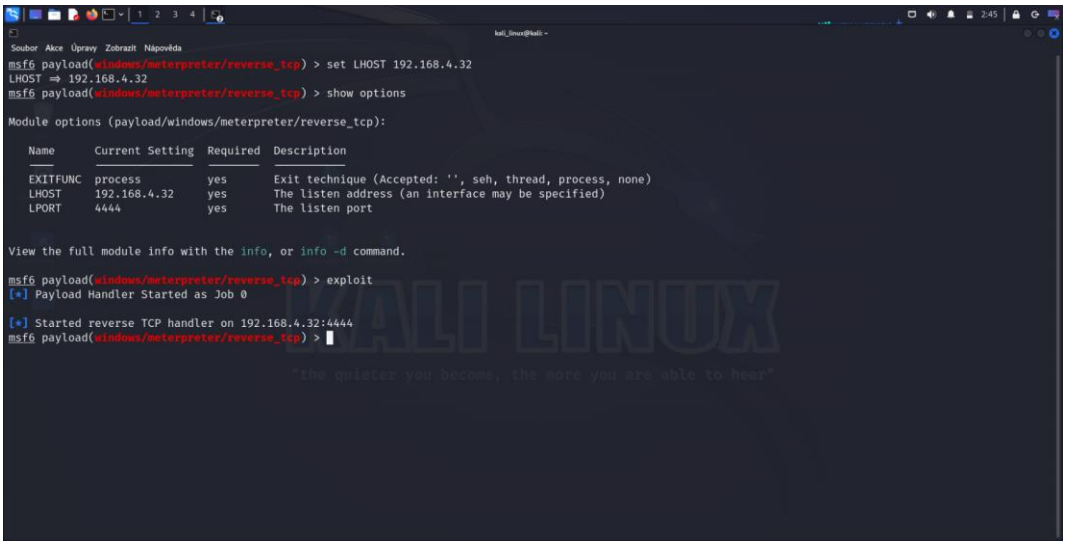


Obrázek 21 Email s přílohou obsahující škodlivý dokument (vlastní).

Po vytvoření archivu již nebyl problém přílohu nahrát do emailu a odeslat. Jelikož je velikost odesílaných souborů limitována, je využívání archivů běžnou praxí. To může platit i v případě dokumentů jako je životopis, kdy může být velikost dokumentu ovlivněna kvalitou vložené fotografie. V případě malwaru je archivace jedním z možných způsobů vyhnutí se detekci antivirovým skenem. Komprimovaná struktura dat je totiž odlišná vůči

původní. Pokud tak nemá antivirový program povoleno rozbalování archivů, může se stát, že škodlivý kód nebude detekován.

Krom zaslání samotného souboru obsahujícího škodlivý kód, který v tomto případě má za úkol navázat spojení se zařízením útočníka, je třeba nastavit proces (dále jen listener), který bude mít za úkol toto spojení zachytit. Víceméně se jedná o komunikaci klient → server, jak je tomu např. u webových služeb. Pro tyto účely jsem zvolil „exploit/multi/handler“, který krom zachycení spojení je schopen operovat s různými payloady. Jako payload jsem pak použil „windows/meterpreter/reverse_tcp“. Jedná se o payload, který má za úkol navázání reverzního shellu komunikujícího pomocí protokolu TCP za použití meterpreteru[13]. Tento payload je tzv. stager. Payloady typu stager se vyznačují malou velikostí a na cílovém zařízení běží v operační paměti, čímž jsou odolnější vůči detekci. Po nastavení listeneru pomocí příkazu „use exploit/multi/handler“ a payloadu pomocí příkazu „set payload/windows/meterpreter/reverse_tcp“ je třeba nastavit parametry tohoto listeneru, viz Obrázek 22.



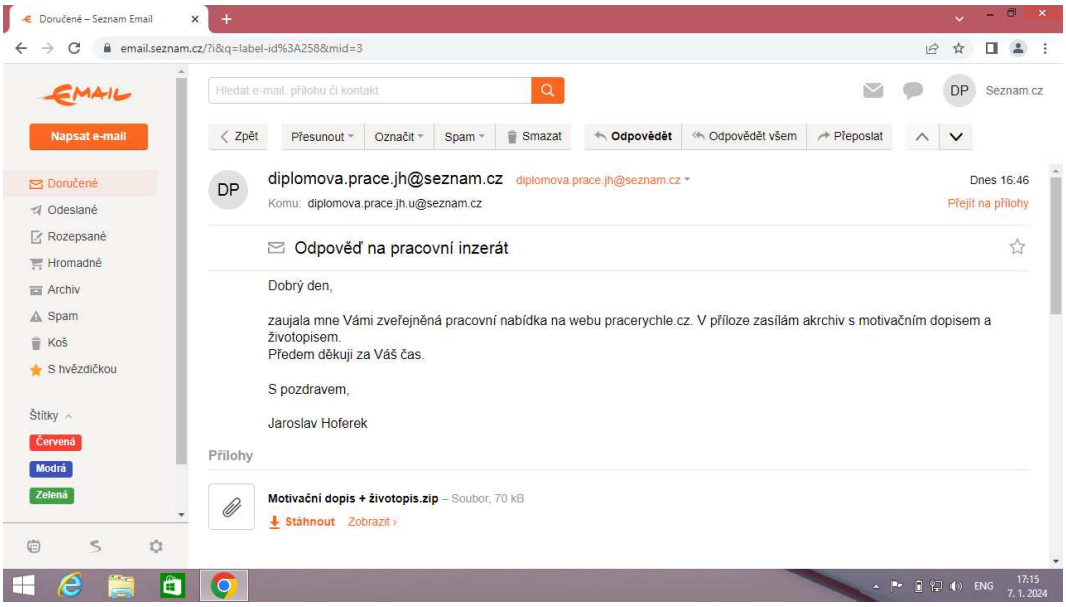
Obrázek 22 Nastavení a spuštění listeneru (vlastní zpracování v Metasploit Framework).

Po nastavení listeneru či C2 serveru, který bude očekávat příchozí spojení, stačí vyčkat, zda oběť otevře infikovaný soubor a provede se implementované makro. V této fázi se přesuneme na stranu oběti, kterou je v kontextu scénáře Paní Zdena.

Paní Zdena, jelikož v předešlých dnech inzerovala pracovní nabídku na pozici seřizovače CNC strojů, očekává odpovědi v podobě emailů s přiloženými životopisy a motivačními

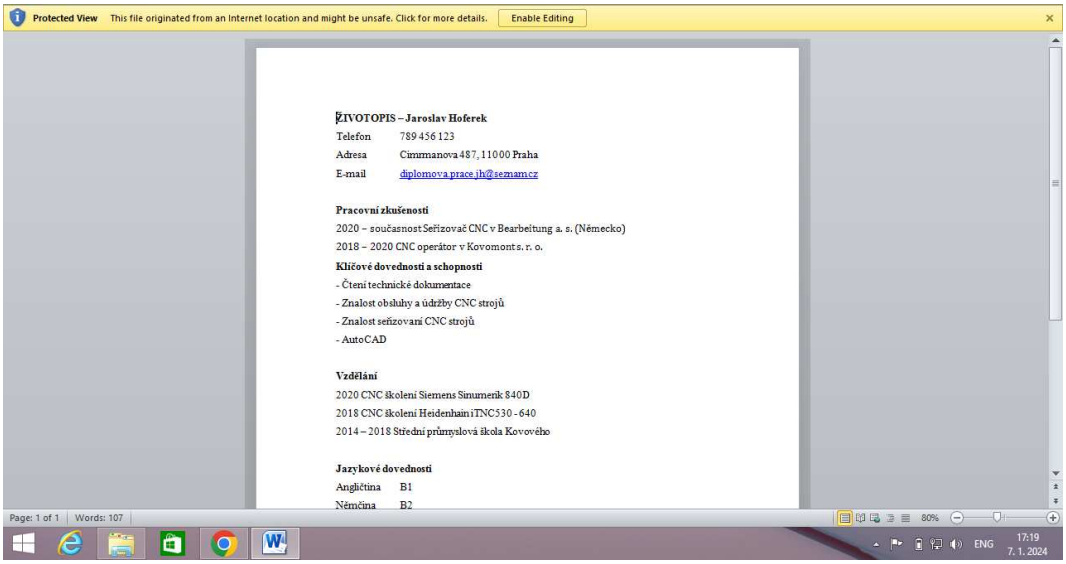
[13] Meterpreter: jedná se o druh payloadu vykonávaný v paměti zařízení, kterým Metasploit disponuje. Meterpreter umožňuje interakci s napadeným zařízením a zadávání základních příkazu či vykonávání kódu.

dopisy od případných zájemců. Tento fakt značně nahrává útočníkovi, jelikož je zde odstraněna jedna z překážek, která by mohla v oběti vyvolat podezření, a sice, že se nejedná o neočekávaný email. Dalším faktem, který může být pro útočníka přínosný, je potenciální množství emailů podobného typu, mezi kterými se bude nacházet i ten s infikovanou přílohou. Rutinní procházení „stejných" emailů může vést také ke snížení pozornosti a případným chybám. Po doručení emailu tedy paní Zdena stáhla přílohu, aby mohl a extrahovat soubory uvnitř archivu, viz Obrázek 23.



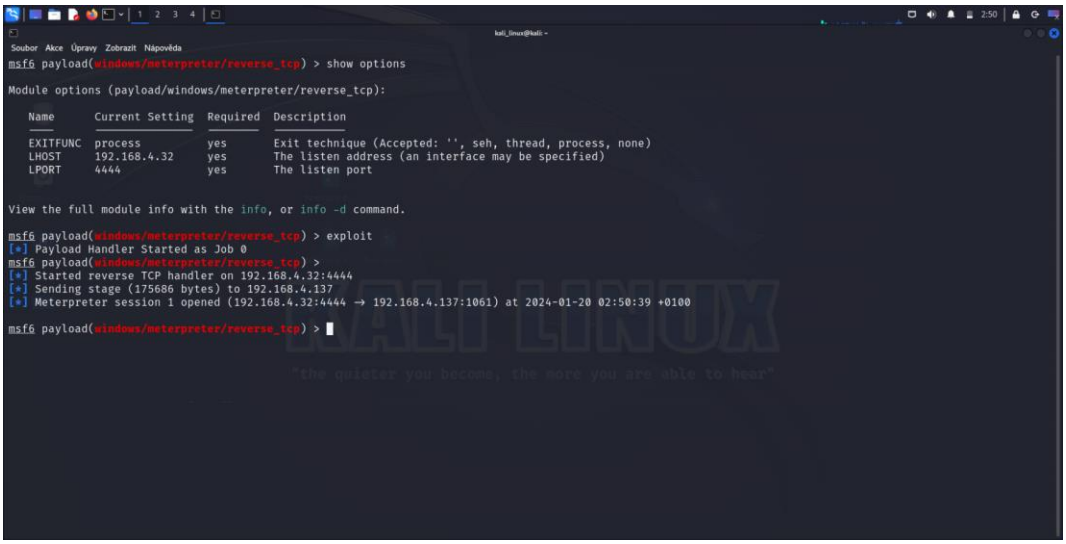
Obrázek 23 Doručený email se škodlivou přílohou (vlastní).

Jak již bylo zmíněno výše, ani příloha v podobě archivu nemusí nutně v oběti vzbudit podezření, jelikož emailové zprávy jsou limitovány určitou velikostí, a proto je zcela běžné, že soubory většího formátu (jehož příčinou může být např. přiložená fotografie) bývají zabaleny do archivů. Po rozbalení archivu mohla paní Zdena rovnou otevřít přiložené soubory. V případě souboru obsahujícího životopis s připojeným škodlivým makrem je však nutné učinit poslední krok před tím, než bude zaslán požadavek z počítače oběti o navázání spojení se zařízením útočníka. A to kliknout na tlačítko „povolit editaci" či „povolit makra", viz Obrázek 24, čímž dokument, který byl doposud otevřen v režimu „čtení", získá možnost všech jeho funkcí, mezi které krom provádění úprav spadá i vykonání maker.



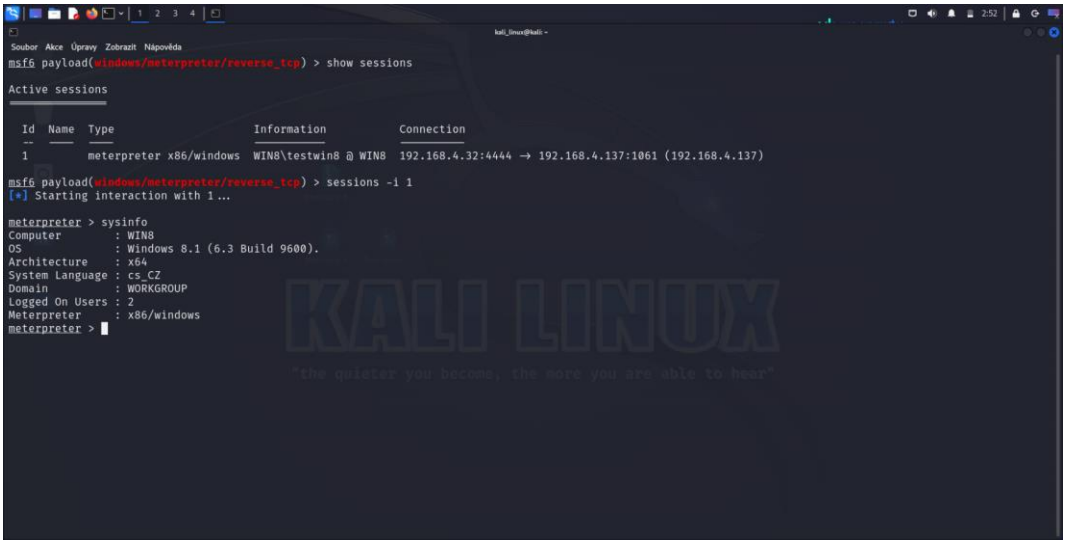
Obrázek 24 Doručený životopis obsahující škodlivé makro (vlastní).

Po kliknutí na tlačítko na horní liště „Enable Editing“, se spustí implementované makro, které zašle požadavek o navázání spojení na IP adresu a port, které jsme nastavili při tvorbě dokumentu. Jelikož je zde nastaven listener, který příchozí spojení očekává, dojde k navázání spojení mezi oběma zařízeními, viz Obrázek 25.



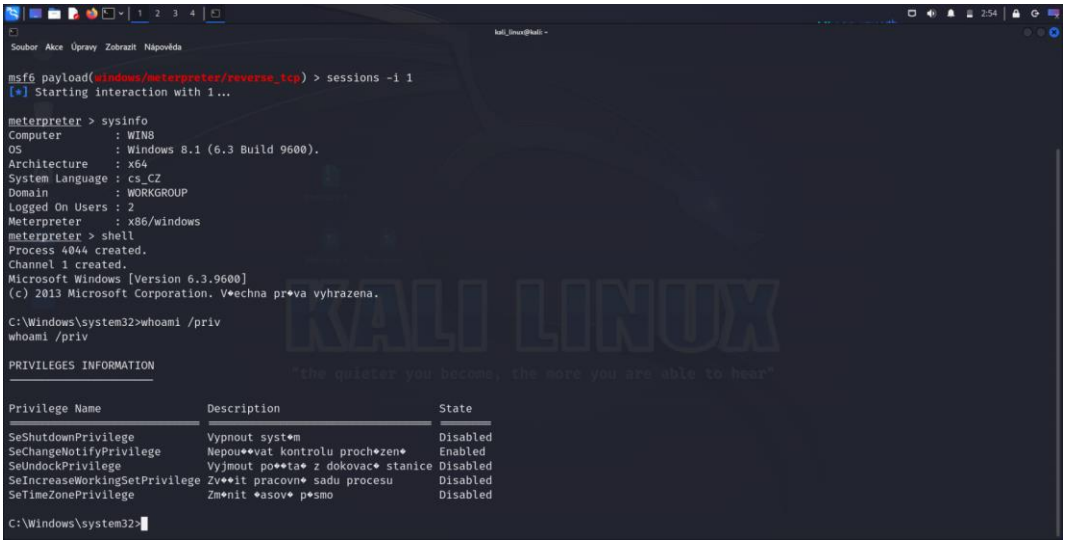
Obrázek 25 Navázání spojení mezi zařízením oběti a útočníka (vlastní zpracování v Metasploit Framework).

Nyní, když bylo spojení úspěšně navázáno, může útočník interagovat se systémem oběti. Pro zobrazení navázaných spojení je možné použít příkaz „show sessions “, který vypíše všechny dostupné spojení v rámci Metasploitu. Pro možnost interakce se zařízením, se kterým je spojení navázáno pak slouží příkaz „sessions – i <id>“, viz Obrázek 26. V tomto případě komunikujeme s napadeným zařízením skrze meterpreter, který byl použit jako payload v rámci nastavení listeneru.



Obrázek 26 Interakce se zařízením oběti skrze meterpreter (vlastní zpracování v Metasploit Framework).

Meterpreter disponuje vlastní sadou příkazů, jejichž výčet je možné získat pomocí příkazu „help“. Vzhledem ke způsobu provedení útoku zde získává útočník první možnost sběru informací o napadeném systému, viz Obrázek 27.



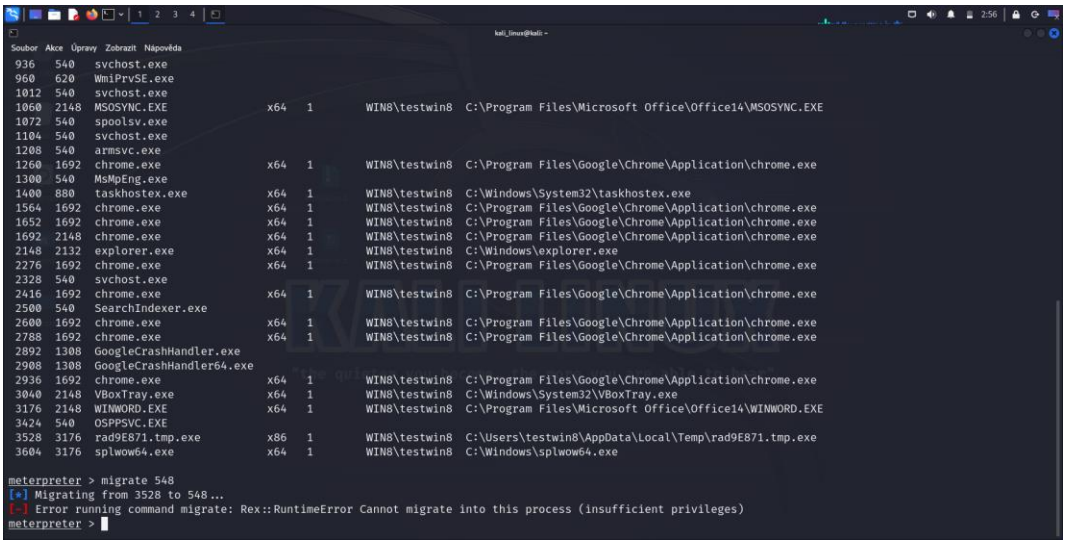
Obrázek 27 Sběr základních informací o systému a účtu oběti (vlastní zpracování v Metasploit Framework).

Na obrázku výše můžeme vidět základní informace, které poskytují útočníkovi přehled o napadeném systému a uživatelském účtu. Útočník tak může na základě zjištěných informací o systému dohledat, zda byly u této verze systému zjištěny nějaké zranitelnosti, kterých by mohl využít v rámci dalšího postupu. Taktéž výpis práv, který je výstupem posledního příkazu na obrázku 26, poukazuje na to, že se jedná o běžný uživatelský účet. Pro provádění akcí jako jsou instalace software či manipulace s procesy souvisejícími

se systémem bude útočník potřebovat vyšší oprávnění, kterými disponuje administrátor či samotný systém.

4.5 Eskalace práv a zajištění perzistentního přístupu

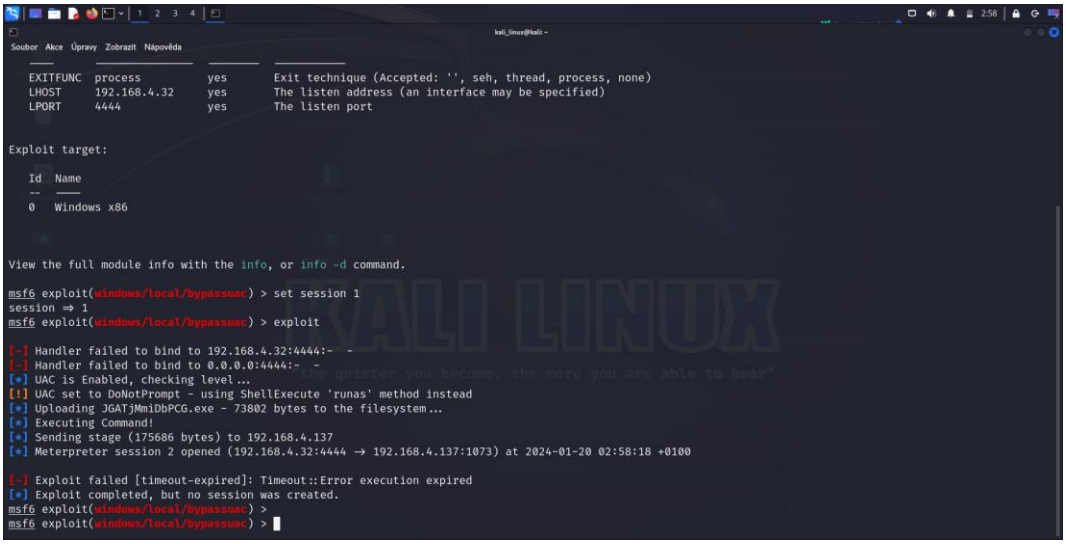
I když je v případě tohoto typu útoku získání přístupu do zařízení oběti stěžejní, neméně důležité je, aby si útočník tento přístup zajistil opakovaně. Jelikož k navázání spojení je třeba spuštění makra uvnitř souboru, v případě ztráty spojení by musela oběť znovu otevřít infikovaný soubor a spustit makro. Na tuto možnost se však není možno spolehnout, proto si útočníci vytvářejí v systému backdoors, které jim umožňují opakovaný přístup. Backdoors mohou mít mnoho podob, např. samospustitelný proces při startu systému, který naváže spojení s útočníkem, vytvoření nového uživatele v systému, či zneužití zranitelnosti některé služby běžící v systému. Pro většinu těchto úkonů je však třeba vyšších práv, jelikož se jedná o instalaci nového softwaru, manipulaci s procesy, na které se vztahují restrikce z hlediska bezpečnostních politik, či vytváření a úpravu procesů souvisejících se systémem. V takovém případě je třeba, aby, pokud takovými právy již uživatel napadeného systému nedisponuje, útočník svá práva povýšil (dále jen eskaloval). Pokud se vrátíme k předchozí kapitole, v jejím závěru útočník zjistil, že účet, ke kterému získal přístup, má práva na úrovní „user“, což jsou běžná uživatelská práva, která samotná nejsou dostačující pro vykonání zamýšlených akcí, viz Obrázek 28. Zde se útočník pokusil migrovat z původního procesu představujícího navázané spojení na proces, který běží v rámci systému a disponuje vyššími právy. V případě úspěchu by tak útočník mohl vykonávat akce „jménem“ tohoto procesu.



Obrázek 28 Zkouška migrace na proces s vyššími právy (vlastní zpracování v Metasploit Framework).

4.5.1 Eskalace práv pomocí exploitu

V důsledku nedostatečného oprávnění napadeného účtu však není tato migrace možná, proto je třeba eskalovat práva. Toto se většinou děje skrze exploitaci zranitelnosti nějaké služby či procesu v rámci systému, kdy v případě úspěchu převezme útočník kontrolu nad tímto procesem či službou i s jejími právy. V tomto případě se exploit pokusí spustit nový shell jako administrátor. Tento shell tak bude disponovat i administrátorskými právy. Tak jako v případě vytvoření souboru či listeneru, i zde je třeba vybrat a nastavit vhodný exploit, příp. payload, který bude použit proti navázanému spojení, viz Obrázek 29.



Obrázek 29 Použití exploitu pro eskalací práv (vlastní zpracování v Metasploit Framework).

Jak můžeme vidět výše, po úspěšném provedení exploitu byla vytvořena nová session/relace s ID 2. Pokud bychom si nyní nechali pomocí příkazu „sessions – i“ vypsat do konzole výčet navázaných spojení, viděli bychom právě dvě aktivní spojení. Pod ID 1 by bylo původní spojení, kde útočník disponuje právy běžného uživatele, pod ID 2 by pak bylo spojení, které představuje nově vytvořený shell s administrátorskými právy. Pokud tedy pomocí příkazu „sessions -i 2“ přejdeme do interakce se zařízením oběti, můžeme si stejným způsobem, jako tomu bylo po navázání spojení, zkontrolovat jakými právy účet, pod kterým relace běží disponuje, viz Obrázek 30.

Obrázek 30 Kontrola práv po eskalaci (vlastní zpracování v Metasploit Framework).

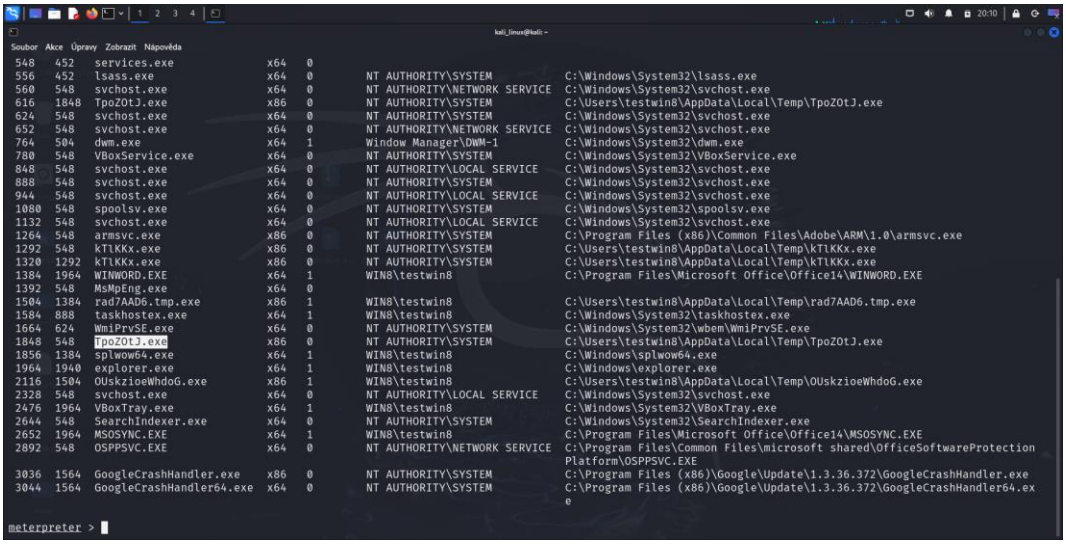
Jak můžeme vidět výše, po úspěšném provedení eskalace již útočník disponuje silnými právy v rámci napadeného systému, které mu umožňují provádění většiny akcí. Dosažení tohoto bodu je důležité pro další postup, kterým bude vytvoření persistentního přístupu do systému. Jak bylo zmíněno na začátku kapitoly, tento krok je důležitý pro zajištění opakovaného přístupu do systému, jelikož momentální navázaná spojení mohou být ztracena, např. v důsledku restartu systému.

4.5.2 Vytvoření persistentního přístupu

Tak jako u předchozích interakcí, i zde musíme zvolit vhodný exploit a payload, skrze které bude zajištěn opakovaný přístup do napadeného systému. Zde použitý exploit dopraví do napadeného počítače spustitelný soubor (.exe), který bude zařazen mezi soubory a skripty, které jsou spouštěny při startu systému. Tento krok není běžnému uživateli z důvodu bezpečnosti umožněn. Jelikož se však v předchozím kroku povedlo eskalovat práva na úroveň administrátora, je útočníkem tato překážka překonána. Jako payload, který bude implementovaným souborem spuštěn je opět reverzní shell, jako tomu bylo u předchozích akcí. Zde je však třeba zadat nový port, na který bude zaslán požadavek o vytvoření spojení, jelikož původní port je stále využíván aktuálním spojením. Dalším parametrem, který je třeba nastavit, je opět session. Zde však musíme zvolit ID odpovídající spojení, ve kterém jsou práva eskalována, viz Obrázek 31.

Obrázek 31 Vytvoření perzistentního spojení s napadeným systémem (vlastní zpracování v Metasploit Framework).

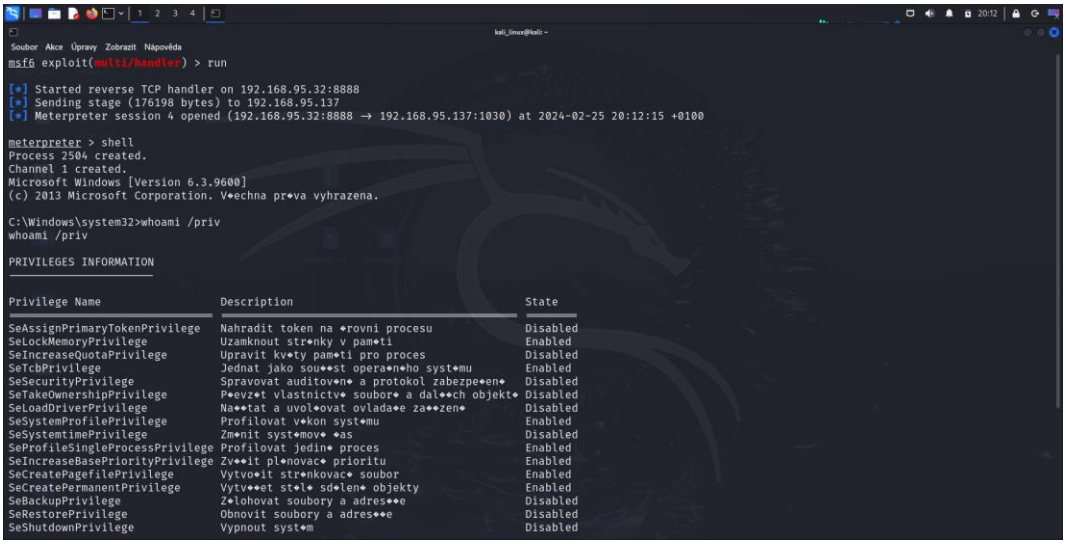
Po spuštění exploitu je v napadeném systému vytvořen spustitelný soubor, který spuštěním payloadu vytvoří v systému nový proces, který naváže spojení se systémem útočníka, viz Obrázek 32.



Obrázek 32 Kontrola vytvoření nového procesu v rámci systému (vlastní zpracování v Metasploit Framework).

Výše pomocí příkazu „ps“ byly vypsány procesy, které běží v rámci napadeného systému. Zde pod číslem 1848, můžeme vidět proces, který byl vytvořen spuštěním implementovaného souboru. Právě tento proces je odpovědný za vytvoření reverzního shellu se zařízením útočníka. Na obrázku (viz Obrázek 33) je vidět znovunavázání spojení se zařízením útočníka, které bylo automaticky navázáno po restartu či opětovném spuštění systému oběti. Jediné, co zde musel útočník zajistit, byl listener, který byl nachystán

naslouchat na adrese a portu, odpovídající nastaveným parametrům v rámci payloadu. Útočník tak získal výchozí bod, ze kterého může sbírat informace či pronikat dále do sítě a systémů v rámci napadené firmy.



Obrázek 33 Automatické navázání spojení po restartu systému oběti
(vlastní zpracování v Metasploit Framework).

4.6 Získání přístupových údajů k účtům napadeného systému

Jednou z akcí, kterou může útočník po získání systému a příslušných práv provést, je sběr informací v napadeném systému. Výše byl sběr prováděn za účelem poznání prostředí, ve kterém se útočník nachází, na základě kterých mohl získat větší kontrolu nad systémem. Jak bylo zmíněno dříve, takto vytvořené zázemí je pro útočníka dobrým výchozím bodem k provádění dalších akcí, a to jak za účelem dalšího postupu v rámci sítě, tak i pro získávání dat a jejich následný prodej. K takovýmto datům patří i údaje v podobě přihlašovacích údajů. Pokud by tak útočník chtěl získat přihlašovací údaje k emailu oběti či další službě, mohl by využít spyware (např. keylogger), pomocí kterého by získal záznamy o stisknutích jednotlivých kláves. Zde by však musel útočník čekat, až na provedení příslušných akcí ze strany oběti. Dalšími údaji, které lze získat, jsou přihlašovací údaje k účtům v rámci systému. Tyto údaje umožní útočníkovi se přihlašovat k účtům jiných uživatelů, získávat zde data a šířit se dál v rámci organizace.

4.6.1 Získání hashů hesel z napadeného systému

Pokud se krátce vrátíme k předchozí kapitole, kde útočník eskaloval práva a vytvořil si persistentní přístup do systému oběti, může rovnou „vytěžit“ ze systému i přihlašovací údaje k uživatelským účtům. V rámci meterpreteru lze tento krok provést za použití příkazu

„hashdump“. Tento příkaz načte do paměti data z příslušného souboru, kde jsou ukládány přihlašovací údaje lokálních uživatelských účtů, viz Obrázek 34.

Obrázek 34 Získání hashů hesel k uživatelským účtům v rámci napadeného systému (vlastní zpracování v Metasploit Framework).

Jelikož se zde jedná o operační systém windows, základním souborem pro ukládání hesel k lokálním účtům je soubor SAM (Security Accounts Manager). Jak můžeme vidět na obrázku, hesla zde nejsou uložena v čisté podobě, ale ve formě hashe. Pokud není nastaveno jinak, umístění tohoto souboru bychom nalezli zde „C:\Windows\System32\config\SAM“, pro systémy Linux „/etc/shadow“. Pro přístup k těmto souborům je vždy zapotřebí vyšších oprávnění, ideálně na úrovni administrátora či systému. V jiném případě bez těchto práv není možné se soubory jakkoliv manipulovat. Každý z operačních systémů také ukládá hashe v jiném formátu. Zde jsou hashe uloženy ve formátu NTLM. Identifikace formátu či algoritmu, který byl pro vytvoření hashe využit, je důležitým předpokladem pro následující kroky v podobě prolomení hashů a získání hesel k daným účtům.

4.6.2 Prolomení hashů pomocí slovníkového útoku

Pro prolomení takto získaných údajů lze využít mnoho různých nástrojů a metod, případně si vytvořit vlastní skript. V tomto případě však využijeme nástroj „hashcat“, který je již součástí Kali Linuxu. Hashcat je nástroj, který je v rámci Kali Linuxu využíván k prolamování hesel. Pomocí tohoto nástroje můžeme provést tzv. „brute force attack“, kdy dochází ke generování náhodných znaků do doby, než se hash vygenerovaný pomocí hashcat shoduje se vzorovým hashem. Rychlost, s jakou je možné tímto způsobem heslo prolomit, záleží na výpočetním výkonu počítače, délce a složitosti samotného hesla. Tato

metoda může být zdlouhavá, proto je většinou proveden pokus o prolomení pomocí slovníku. Slovníkový útok je metodu, kdy útočník využije souboru obsahujícího uniklá či dobře známá hesla a jejich hashe porovná se vzorovým hashem, který získal v systému oběti. Za předpokladu, že slovník obsahuje hledané heslo, je tato metoda nesrovnatelně rychlejší. Pro provedení slovníkového útoku pomocí hashcat potřebuje útočník hashe, které získal v předchozím kroku, uložit do textového souboru ve svém zařízení. Tento soubor pak zakomponuje spolu se slovníkem do příkazu v rámci nástroje hashcat. Po zadání a potvrzení příkazu začne hashcat převádět hesla ze slovníku na zadaný typ hashe (zde -n 1000 značí, že se jedná o NTLM hash), který následně porovná s hashem v zadaném textovém souboru. Pokud bude takto nalezena shoda, k danému hashi se vypíše i heslo, viz Obrázek 35.

Obrázek 35 Prolomení získaných hashů pomocí nástroje hashcat
(vlastní zpracování v hashcat).

S takto získanými údaji může útočník přistupovat v rámci systému k uvedeným účtům, aniž by budil známky podezření ve formě neplatných pokusů o přihlášení se k účtu, které by mohly být zjištěny z příslušných logů v rámci průběžného monitoringu. V tomto scénáři však útočník přístupové údaje prodal, čímž umožnil přístup do organizace i jiným útočníkům, kteří mohou být na vyšší úrovni, což může zvýšit dopady na danou organizaci.

5 PŘÍPRAVA OBLASTÍ ŠKOLENÍ PRO ZVÝŠENÍ ODOLNOSTI UŽIVATELŮ VŮČI PROVEDENÉMU ÚTOKU

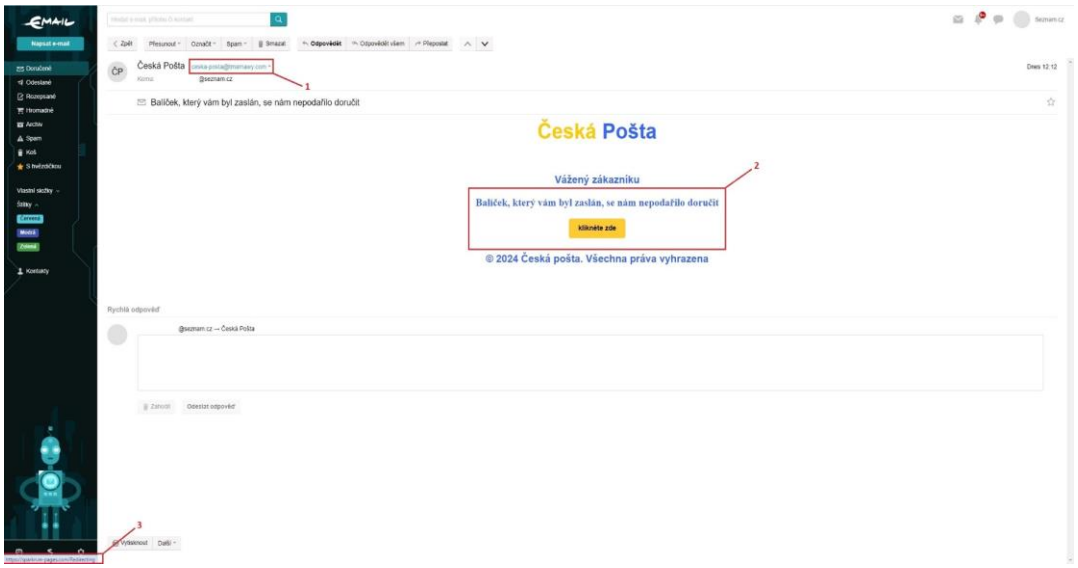
S postupným uvědoměním si důležitosti kybernetické bezpečnosti se ze strany podniků zvyšují i investice do této oblasti. S potřebou držet krok s útočníky a s přílivem financí od zákazníků poptávajících bezpečnostní služby získaly společnosti zabývající se bezpečnostními technologiemi ideální podmínky pro vývoj nových bezpečnostních řešení. I přes veškerý technologický pokrok zůstává člověk významnou komponentou pomyslného bezpečnostního řetězu. Tak jako je tomu i u většiny ostatních oblastí bezpečnosti, i zde je člověk onou pomyslnou „Achillovou patou“. V případě zvýšení bezpečnosti lidského faktoru stále platí, že nejúčinnější ochranou jsou vědomosti. Proto je třeba uživatele řádně seznámit a průběžně aktualizovat jejich povědomí o rizicích, kterým mohou být v kybernetickém prostoru vystaveni. Případy, kdy je firma povinna školit zaměstnance v oblasti kybernetické a informační bezpečnosti, mohou být např. podmínky pro získání osvědčení dle ISO 27001 či splnění požadavků dle stávající i připravované vyhlášky o kybernetické bezpečnosti v případě, že se na firmu vztahuje regulace dle ZoKB.

Pro účinné školení uživatelů je nezbytné, aby byla z jejich strany při jeho provádění věnována plná pozornost. Jak již bylo uvedeno dříve, získání pozornosti posluchačů při školení se může stát pro školitele výzvou. A to zejména vzhledem k odlišným technologickým znalostem. Nedostatek znalostí v oblasti ICT může v posluchačích vyvolávat nezájem o celé školení a zvolení přístupu „nějak to tu odsedím“. Pro upoutání pozornosti a zvýšení zájmu školených osob může posloužit reálný příklad, kterým může být provedení útoku v rámci předcházející části práce. Další způsob získání možného zájmu představuje zahrnutí praktické části jakožto druhé poloviny školení. Praktická část zaměřená na identifikaci podvodných zpráv, základní nastavení systému a zacházení s antivirovými programy či jinými produkty určenými pro běžné uživatele, by měla být prezentována posluchačům jako „co můžu udělat ještě dnes pro svou bezpečnost“. Krom možného získání vyšší pozornosti posluchačů, tak školitel naučí uživatele základním bezpečnostním dovednostem, které mohou použít i v domácím prostředí. Uživatelé ICT technologií, kteří mají základní bezpečnostní návyky v jejich užívání, představují pro firmy menší bezpečnostní riziko, jelikož je zde předpoklad, že i jejich vlastní zařízení, které jsou mnohdy připojovány do firemní sítě, budou lépe zabezpečeny a udržovány. I když je cíleným efektem firemních školení zvýšení bezpečnosti dané firmy, vedlejším účinkem takto prováděných školení je i plošné zvýšení bezpečnosti ve státě. V následujících kapitolách budou

zpracovány jednotlivé body praktické části školení kybernetické bezpečnosti, kdy kompletní školení bude vypracováno jako samostatná příloha diplomové práce.

5.1 Identifikace ukazatelů podvodné zprávy

Nejen pro zaměstnance, ale i běžné uživatele, patří interakce s emaily ke každodenní činnosti. Právě emaily jsou v současnosti jednou z nejrozšířenějších služeb, která je zneužívána útočníky ke krádeži osobních údajů či získání přístupu do zařízeních. Z metod sociálního inženýrství, které jsou útočníky využívány, je phishing tím nejběžnějším, s čím se můžeme setkat. Z tohoto důvodu je nezbytné, aby se uživatelé naučili rozpoznat, zda se jedná o legitimní zprávu, anebo podvod. Kvalita provedení phishingu přímo závisí na schopnostech a znalostech útočníka. Můžeme se tak setkat s emaily, z nichž je hned na první pohled jasné, že se jedná o podvod, ale též s takovými, které jsou téměř k nerozeznání od legitimní zprávy. Na obrázku níže (viz Obrázek 36 a Příloha č. 1) je zobrazen email, který mi byl zaslán „Českou poštou“.

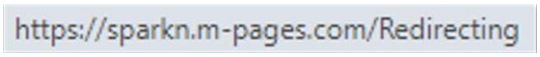


Obrázek 36 Podvodný email vydávající se za Českou poštu (vlastní).

Na obrázku jsou vyznačeny tři body na základě, kterých je možné rozpoznat, že se jedná o podvodný email. Před tím, než se však začneme zabývat přímo jednotlivými body v obrázku, je zde ještě jeden aspekt, který bychom mohli označit jako nultý bod, a to, zda nějaký email od České pošty očekáváme. Již to, že neočekáváme balíček či jsme si k jeho doručení vybrali jiného dopravce, by mělo vzbudit počáteční podezření. Bod č. 1 se zaměřuje na adresu odesilatele emailu, viz Obrázek 37.

Obrázek 37 Adresa odesílatele emailu (vlastní).

Adresa odesilatele emailu v tomto tvaru neodpovídá adrese České pošty, taktéž emailová doména „@tmamawy“ a top doména „.com“ nejsou Českou poštou využívány. Bod č. 2 poukazuje na způsob, jakým je zpráva formulována. Bez jakýchkoli informací o balíčku, je příjemce přímo vyzván ke kliknutí na tlačítko. Toto tlačítko by mělo sloužit k přesměrování na stránku, kde příjemce vyplní nové údaje pro „Českou poštu“. Pokud si však chceme ověřit, kam budeme přesměrováni, stačí kurzorem myši najet na tlačítko (neklikat), kdy se nám zobrazí v levém dolním rohu cílová URL adresa. Tato URL adresa je zaznačena jako bod č. 3. Při jejím detailnějším prozkoumání, viz Obrázek 38, můžeme vidět, že směřuje na stránku, která svým názvem nenaznačuje, že by se mělo jednat o stránku České pošty.



Obrázek 38 Cílová adresa přesměrování (vlastní).

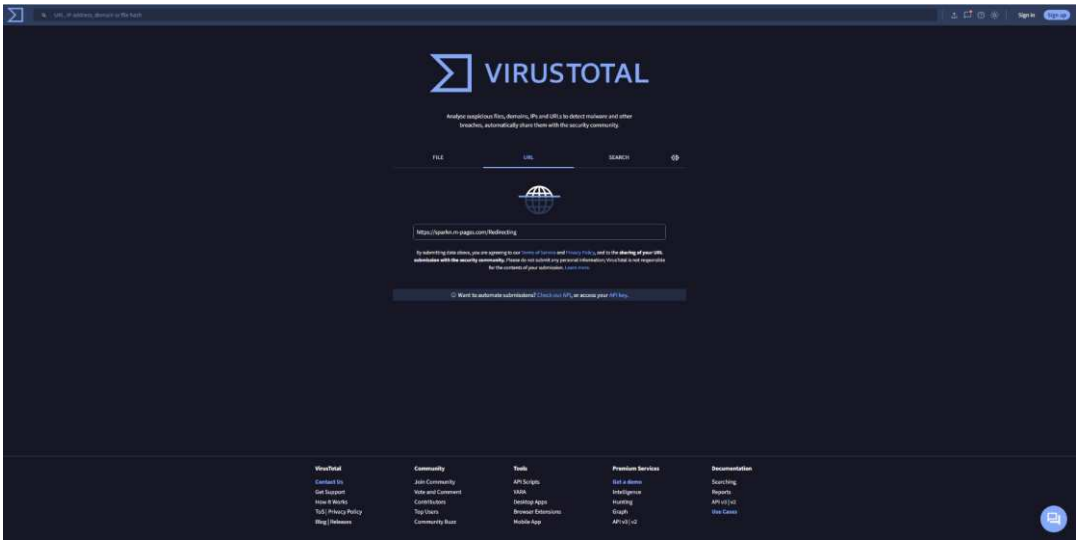
Zde bychom očekávali spíše adresu ve tvaru https://www.ceskaposta.cz/sluzby, která je originálním odkazem portálu České pošty, přičemž text za lomítkem adresy odkazuje na záložku „Služby“ na tomto portále. Pomocí jednoho či všech výše uvedených znaků je možné určit, že se nejedná o legitimní email České pošty, nýbrž o phishing.

5.2 Ověření odkazu a přílohy pomocí nástroje VirusTotal

V případě, že se jedná o phishing vyšší kvality, je mnohdy rozdíl v URL adrese, na kterou je uživatel přesměrován jen v jednom znaku či mezeře. Dalším úskalím mailové komunikace mohou být přílohy, které mohou být využity jako nositel škodlivého kódu či přesměrování na infikovanou stránku. Na rozdíl od emailu, jehož účelem je jen sbírat osobní údaje oběti, zde představuje riziko samotná interakce s přílohou či infikovanou stránkou. Online služba VirusTotal nabízí možnost ověření URL adresy či souboru, kdy je kontrola provedena skrze vícero poskytovatelů bezpečnostních softwarů. Pro účely demonstrace skenu URL adresy bude použit stejný email, jako v předcházející kapitole. Budeme simulovat situaci, jako by výše identifikované body naznačující pokus o phishing neexistovaly, a zpráva by se tak jevila na první pohled jako legitimní.

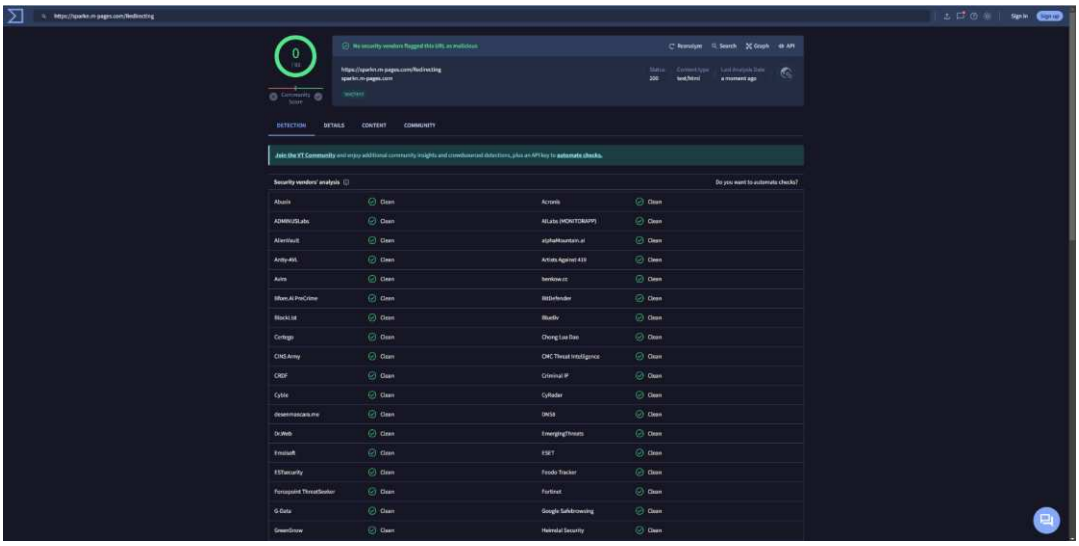
5.2.1 Sken adresy pomocí VirusTotal

Pro získání URL adresy je třeba kliknout pravým tlačítkem myši na tlačítko „klikněte zde“ a vybrat možnost „kopírovat adresu odkazu“. Na stránce https://www.virustotal.com vybereme záložku URL a do řádky vložíme vykopírovaný odkaz, viz Obrázek 39 a Příloha č. 2.



Obrázek 39 Kontrola URL adresy pomocí nástroje VirusTotal
(vlastní zpracování ve VirusTotal).

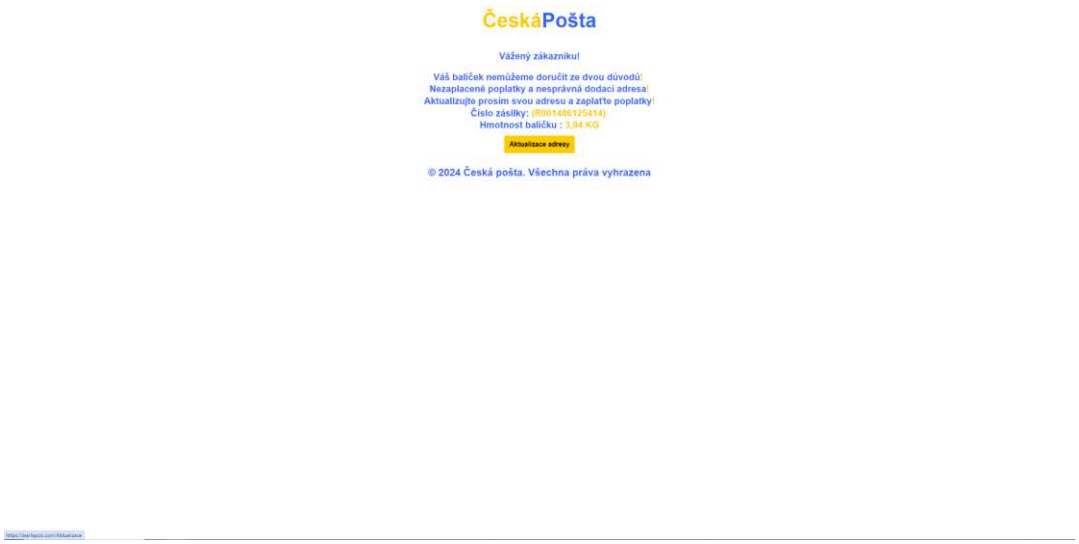
Po zadání a potvrzení adresy v řádce provede VirusTotal kontrolu dané URL adresy. Výsledkem je výstup v podobě skóre značícího kolik z celkového množství poskytovatelů bezpečnostního softwaru shledalo odkaz či soubor jako škodlivý, viz Obrázek 40 a Příloha č. 3.



Obrázek 40 Výsledek prvního skenu URL adresy
(vlastní zpracování ve VirusTotal).

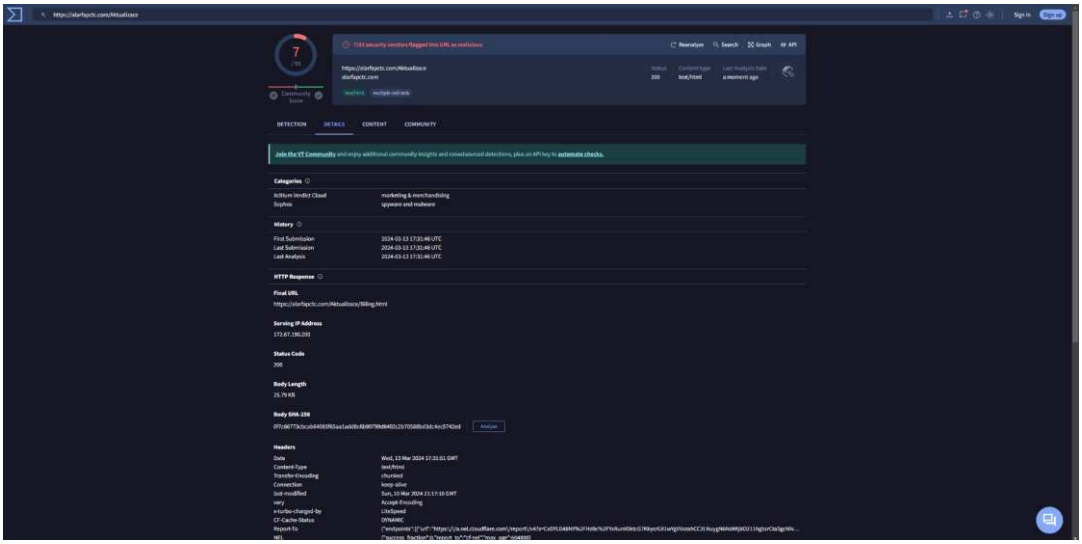
Jak můžeme vidět na obrázku, sken neodhalil žádný nález. Tímto bychom mohli považovat stránku na kterou odkaz směřuje za bezpečnou (výsledky skenu mohou být ovlivněny i unikátností malwaru).

Pokud tedy následně v původním phishingovém emailu klikneme na tlačítko „klikněte zde“, odkaz nás přesměruje na tuto stránku, viz Obrázek 41 a Příloha č. 4.



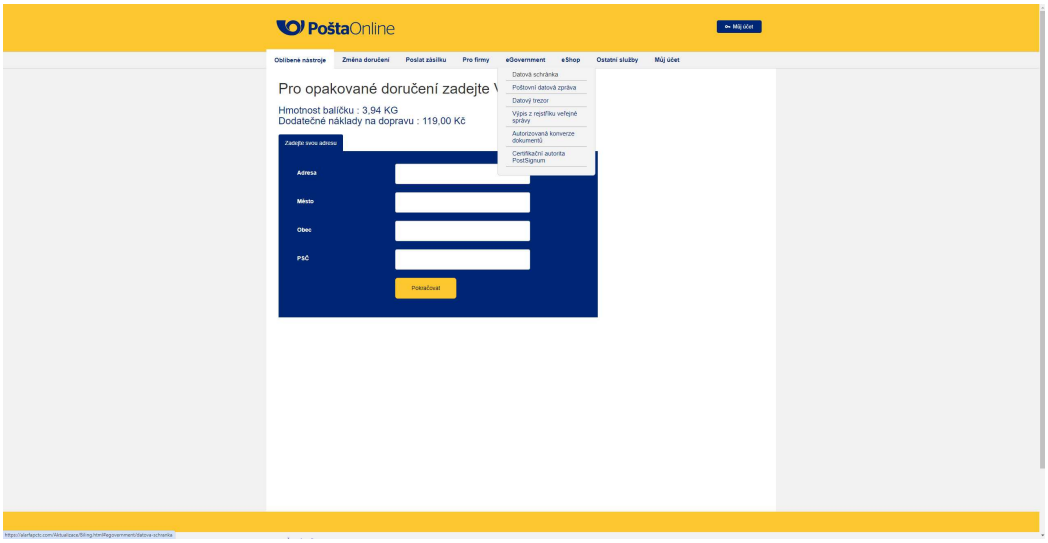
Obrázek 41 První stránka po přesměrování (vlastní).

Cílová stránka, na kterou došlo k přesměrování pomocí tlačítka „klikněte zde“ je podobného charakteru jako původní email. Zde však můžeme vidět i první informace o zásilce. Taktéž charakter textu je oproti prvnímu koncipován tak, aby působil důrazněji. Můžeme si tak povšimnout vykřičníků, které zakončují každý z řádků, a to včetně oslovení. Útočník se tímto snaží na oběť vyvinout nátlak, kdy se snaží vyvolat strach z potenciálních následků nenásledování pokynů ve zprávě (zde by se tak mohlo jednat o případný doplatek). V této fázi krom charakteru zprávy, kterou se útočník snaží vyvinout nátlak, by měl podezření vzbudit i fakt, že odkaz nevedl přímo na portál české pošty. Útočník zde použil tuto stránku jako mezistupeň pro zvýšení odolnosti proti skenům, kterými jsou emaily kontrolovány. Pokud tato stránka (URL adresa) není nahlašována ručně (uživateli), pro skenery se jeví jako neškodná stránka s textem a odkazem. Pokud však podrobíme skenu odkaz, který se skrývá pod tlačítkem „Aktualizace adresy“, dosáhneme již jiných výsledků, viz Obrázek 42 a Příloha č. 5.



Obrázek 42 Výsledek skenu druhého odkazu (vlastní zpracování VirusTotal).

Druhý sken již vyhodnotil odkaz jako škodlivý resp. 7/93 poskytovatelů hlásí tento odkaz jako škodlivý. Pod záložkou „Details“ v kolonce „Categories“ můžeme vidět, do jaké kategorie nález spadá. Pokud bychom tedy klikli na odkaz, byly bychom přesměrováni na stránku, která již svým vzhledem připomíná portál České pošty, viz Obrázek 43 a Příloha č. 6.



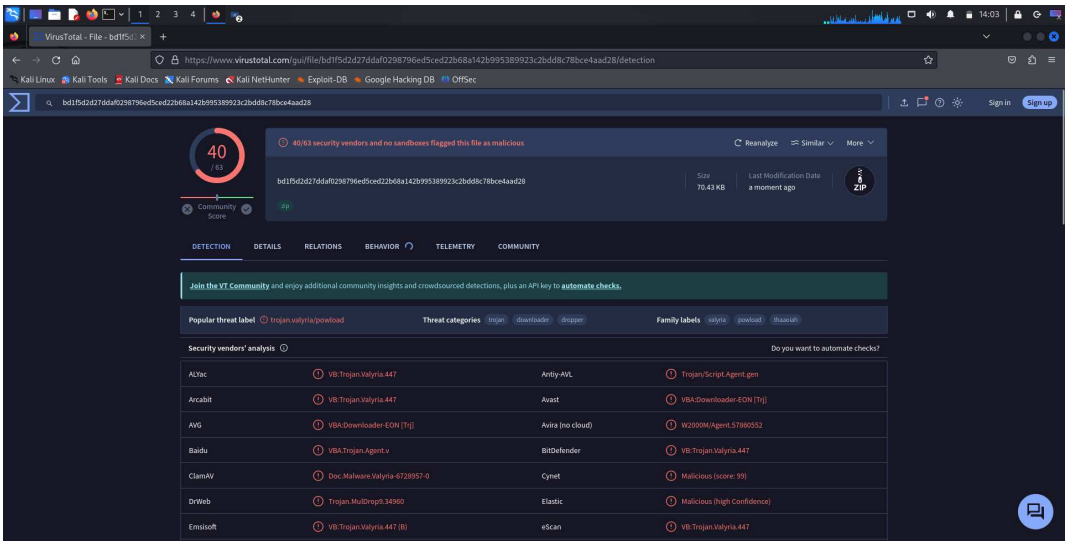
Obrázek 43 Podvodný portál České pošty (vlastní).

Pokud bychom zde zadali údaje o adrese našeho bydliště, byly bychom přesměrováni na další stránku, která by nás vybídla k zaplacení „dodatečných nákladů na dopravu“ ve výši 119,- Kč. Krom zmíněných peněz bychom však přišli i o veškeré zadané údaje, včetně těch platebních. I když se jednalo o poměrně slabý pokus o phishing, bylo možné skrze něj demonstrovat prvky podvodných zpráv a skenování URL adres. Jestliže by byla součástí

emailu i příloha, bylo by ji možné podrobit testu podobně jako URL adresu. V případě testování souborů pomocí online nástrojů bychom měli mít na paměti, že bychom neměli takto testovat soubory, které obsahují citlivá data.

5.2.2 Sken přílohy pomocí VirusTotal

Pro demonstraci skenu souboru byl použit archiv, který byl použit v rámci scénáře předchozí části. Tento archiv obsahuje dva textové soubory, z nichž jeden má v sobě implementované makro, které se po spuštění pokusí navázat spojení se zadanou IP adresou. Ve scénáři, nebyl antivirovým programem nahlášen žádný škodlivý soubor, jelikož cílový systém nebyl aktualizován. Pokud bychom však zkusili sken pomocí VirusTotal, dostali bychom zcela jiný výsledek, viz Obrázek 44 a Příloha č. 7.



Obrázek 44 Výsledek skenu přílohy použité ve scénáři
(vlastní zpracování VirusTotal).

Zde na obrázku můžeme vidět, že 40 z celkového počtu 63 použitých bezpečnostních softwarů zaznamenalo škodlivé chování souboru. Nad použitými bezpečnostními softwary můžeme vidět, že příloha, kterou jsme nechali ověřit byla identifikována jako trojský kůň.

5.3 Více faktorové ověření a správce hesel

Silné heslo je základem v ochraně přístupu k uživatelským účtům. Jeho délka a kombinace znaků snižují šanci na jeho prolomení. S rostoucím výpočetním výkonem, který však mají útočníci k dispozici, klesá i čas potřebný k prolomení hesla. To klade zvýšené nároky na uživatele při tvorbě hesel. Hesla, která obsahují velká a malá písmena, číslice a speciální znaky o délce deseti a více znaků, jsou však pro mnohé těžce zapamatovatelná, zvláště, když pro každý účet by mělo být samostatné unikátní heslo. Seznámení uživatelů se správci hesel,

může zabránit vytváření slabých hesel či opakování jednoho hesla pro více účtů, viz Příloha č. 8.

Zabezpečení přístupů k uživatelským účtům bychom však neměli stavět jen na silném heslu. Pokud z nějakého důvodu dojde k úniku hesla, útočníkovi nic nebrání v přístupu do účtu uživatele. Z tohoto důvodu je vhodným řešením aplikace více faktorového ověření, kdy po zadání správného hesla je třeba se prokázat ještě jiným způsobem. Nejčastějšími metodami je číselný kód zaslaný pomocí SMS či potvrzení přístupu v samostatné aplikaci. Pokud by tedy i došlo k úniku hesla, útočník by se stále nemohl k účtu uživatele přihlásit. V Příloze č. 9 je zobrazena mobilní aplikace Microsoft Authenticator, která krom funkce dvoufázového ověření poskytuje i správce hesel, který byl zmíněn výše. Uvědomění si důležitosti ochrany přístupů v rámci uživatelských účtů ze strany uživatelů je nezbytné nejen pro uživatele samotné, ale i pro firmy, které tyto uživatele zaměstnávají. V případě krádeže uživatelského účtu by mohl být tento účet zneužit útočníkem např. při spear-phishingu.

5.4 Základní zabezpečení sytému Windows pro uživatele

Ať už po instalaci operačního systému či v průběhu jeho používání by měl uživatel dbát na udržování zařízení v bezpečném stavu. Tento proces bychom mohli rozdělit do čtyř bodů:

1. Udržování aktuálnosti systému a aplikací.
2. Řízení uživatelských účtů (UAC).
3. Zajištění adekvátní antivirové ochrany.
4. Držení jen těch aplikací, které jsou využívány.

5.4.1 Aktualizace systému

Udržování operačního systému a aplikací v aktuálním stavu je jedním ze základních prvků bezpečnosti zařízení. Zde je třeba, aby uživatelé pochopili celkový význam aktualizací, a to, že se nejedná jen o prostředek k optimalizaci výkonu aplikace či přidání nové funkce, ale jedná se také o nástroj pro implementaci „záplat“ zjištěných zranitelností. V případě antivirového softwaru je také pomocí aktualizací doplněna databáze, na základě které software rozpozná škodlivý kód. Pro zajištění stálé aktuálnosti systému je vhodné nastavit tento proces jako automatický. V systému Windows 10/11 je možné tento krok provést v „Nastavení → Windows Update“, kde zaznačíme příslušnou kolonku, viz Příloha č. 10.

5.4.2 Řízení uživatelských účtů

User Account Control neboli UAC slouží k řízení uživatelských účtů. Jedná se o formu ochrany, kdy aplikace, která při úkonu potřebuje administrátorská práva, je v jejich zpřístupnění zastavena a potřebuje schválení uživatele. Správné nastavení UAC tak může zabránit eskalaci práv při napadení systému či spuštění škodlivého kódu (viz kapitola 4.5). Nastavení UAC lze provést ve Windows v „Ovládací panely → Systém a zabezpečení → Zabezpečení a údržba → Změnit nastavení nástroje Řízení uživatelských účtů“, viz Příloha č. 11.

5.4.3 Antivirová ochrana

Antivirová[14] ochrana je nezbytným doplňkem nejen počítačů, ale i dalších zařízení, jako jsou např. tablety a mobilní telefony. Existuje mnoho dodavatelů bezpečnostních softwarů, které si mohou uživatelé pořídit za poplatek či jako open-source. Antivirové programy zajišťují kontrolu systému před škodlivým kódem při běhu systému, a to jak kontrolou nových souborů, tak i těch stávajících, které se nachází na disku. V závislosti na poskytovateli a úrovni produktu je tento software schopný poskytovat i další způsoby ochrany, jako je např. kontrola v reálném čase či IDS. Uživatel je tak chráněn nejen proti hrozbám cílícím na souborový systém zařízení, ale i v rámci spojení skrze procházení webových stránek či lokální sítě. Windows 10 a 11 disponuje vlastním integrovaným řešením v podobě Microsoft Defender, který je instalován zároveň se systémem. Microsoft Defender je plnohodnotný antivirový software, který je schopný fungovat samostatně či společně s antivirovým řešením jiného dodavatele. I když antivirové programy fungují většinu času automaticky, je žádoucí provádět i manuální skenování systému, kdy uživatel zvolí pokročilejší možnosti skenování. Microsoft Defender nabízí čtyři druhy kontroly, viz Příloha č. 11:

1. Rychlá kontrola.
2. Úplná kontrola.
3. Vlastní kontrola.
4. Kontrola programem Microsoft Defender Offline.

Zatím co u prvních třech bodů je jejich účel jasný, sken, který je uveden v bodu čtyři, je mnohdy opomíjen. Tento sken (u jiných výrobců uváděn např. jako sken po restartu) se

[14] Pro účely práce budou pojmy Anti-malware a Antivirus brány jako ekvivalentní pojmy.

zaměřuje na kontrolu procesu, který předchází samotnému načtení operačního systému. Malware, který se soustředí na nižší úrovně zařízení, než je operační systém, totiž nedokáže běžný sken odhalit, jelikož běží na nižší úrovni než ostatní procesy či pozmění hlavní spouštěcí záznam (MBR). Pokud by tak došlo k infekci zařízení např. pomocí rootkitu, mohl by útočník dlouhodobě zneužívat zařízení, aniž by byl odhalen. Jelikož automatické skeny jsou prováděny většinou pomocí „Rychlé kontroly“, je třeba průběžně provádět skeny ručně pomocí kontroly v bodech 2 a 4.

5.4.4 Správa aplikací

Správa aplikací je mnohdy opomíjená, avšak důležitá komponenta zabezpečení zařízení. Krom zajištění aktualizací bychom měli v zařízení mít jen ty aplikace, které využíváme. Realita je však mnohdy zcela jiná, kdy na rozhodování, kterou aplikaci odinstalujeme dochází až v okamžiku, kdy dochází na disku místo a koš je již vysypaný. Na aplikace instalované v systému je však třeba pohlížet, jako na potenciální přístupový bod do systému. A sice v případě, že by instalovaná aplikace obsahovala chybu, kterou by útočník či malware mohl zneužít k získání přístupu do systému či jiných aktivit mířených proti uživateli. Krom samotného počtu držených aplikací zvyšující množství potenciálních zranitelností je zde také fakt, že pokud aplikaci nevyužíváme, nedochází k instalaci vydaných aktualizací. V rámci seznamování uživatelů se zabezpečením jejich zařízení, by neměl být tento fakt opomenut.

ZÁVĚR

Zavádění a udržování kybernetické bezpečnosti v organizacích a firmách zvýšilo poptávku po odbornících v dané oblasti. Realitou však je, že je těchto odborníků nedostatek. Firmy jsou proto nuceny delegovat úkoly mezi členy oddělení informačních technologií, jejichž odbornost se nachází více v budování a správě informační infrastruktury. Právě při správě infrastruktury lze provádět i skeny zranitelností. I pro tyto účely může být využit nástroj Metasploit, který byl představen v první polovině praktické části. V rámci činností IT oddělení tak může posloužit, jako doplňkový nástroj pro otestování nově implementovaných technologií či jako předstupeň odborného testování.

Jako výstup práce je zpracován materiál pro školení uživatelů/zaměstnanců, který krom předání základního povědomí o oblasti kybernetické bezpečnosti a hrozbách v kybernetickém prostoru, poskytuje i ukázky, jak si mohou následně i sami uživatelé zajistit alespoň základní ochranu vlastních zařízení. Toto pak může být počátečním impulzem, na základě kterého bude uživatel dále rozvíjet své povědomí, a budovat si bezpečnostní návyky v užívání ICT zařízeních a bezpečného pohybu v kybernetickém prostoru. Tento materiál je ve formě PDF přílohy a je určen k volnému použití. Obsah je obecného charakteru, proto pokud by měl být použit pro školení ve firmě či společnosti, je vhodné jej doplnit o poznatky z dané firmy.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI Artificial intelligence

APT Advanced Persistent Threat

BIOS Basic Input-Output System

CaaS Cybercrime as a Service

CLI Command Line Interface

DDoS Distributed Denial Of Service

DoS Denial Of Service

GUI Graphic User Interface

IaaS Infrastructure as a Service

ICT Information and Comunication Technology

IDS Intrusion Detection System

ISMS Information Security Management Systém

IP Internet Protocol

IPS Intrusion Prevention System

IT Information Technology

SaaS Software as a Service

SMB Server Message Block

LAN Local Area Network

MaaS Malware as a Service

MBR Master Boot Record

ML Machine learning

NaaS Network as a Service

OSINT Open Source Inteligence

PaaS Platform as a Service

PaaS Phishing as a Service

UAC User Acces Control

URL Uniform Resource Locator

VM Virtual Machine

ZoKB Zákon o kybernetické bezpečnosti

SEZNAM LITERATURY

ADLAM, Stephanie, 2023. *Infostealer Malware: Top Stealers in 2023*. Online. GRIDINSOFT.COM. GridinSoft. Dostupné z: https://gridinsoft.com/blogs/infostealer-malware-top/. [cit. 2023-10-27].

A. NETTLES, Roderick; MERULLA, Charlie a WARZALA, Steve, 2019. *Data Manipulation: Attacks and Mitigation*. Online. CSIAC: Cybersecurity & Information Systems Information Analysis Center. Dostupné z: https://csiac.org/articles/data-manipulation-attacks-and-mitigation/. [cit. 2024-01-05].

AYCOCK, John, 2006. *Computer viruses and malware*. 1. Canada: Springer. ISBN 9780387302362.

BAKER, Rae, 2023. *Deep Dive: Exploring the Real-world Value of Open Source Inteligence*. 1. New Jersey: Wiley. ISBN 978-1-119-93324-3.

BARRETT, Jonathan, 2022. *What Are the Types of Ransomware Attacks?* Online. VECTRA. Dostupné z: https://www.vectra.ai/blog/what-are-the-types-of-ransomware-attacks. [cit. 2024-04-08].

BASUMALLICK, Chiradeep, 2023. *What Is the Internet? Meaning, Working, and Types*. Online. Spiceworks. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-the-internet/. [cit. 2024-03-05].

BAZZELL, Michael, 2023. *OSINT TECHNIQUES: RESOURCES FOR UNCOVERING ONLINE INFORMATION*. 10. Independently Published. ISBN 9798366360401.

BELCIC, Ivan a NELSON, Brittany, 2021. *What Is the Dark Web and How to Access It?* Online. Avast. Dostupné z: https://www.avast.com/c-dark-web. [cit. 2024-03-06].

BUCKBEE, Michael, 2022. *What is Metasploit? The Beginner's Guide*. Online. Varonis. 24. 2. 2022. Dostupné z: https://www.varonis.com/blog/what-is-metasploit. [cit. 2024-01-08].

BUNTZ, Brian, 2013. *A CIA-Inspired Approach to Medical Device Cybersecurity*. Online. In: Mddionline.com. Dostupné z: https://www.mddionline.com/software/a-cia-inspired-approach-to-medical-device-cybersecurity. [cit. 2024-01-02].

ČERMÁK, Miroslav, 2014. *Informační bezpečnost vs. kybernetická bezpečnost*. Online. In: Cleverandsmart.cz. Dostupné z: https://www.cleverandsmart.cz/information-security-vs-cybersecurity/. [cit. 2024-01-01].

DHOLAKIYA, Pratik, 2021. *What Is the Cyber Kill Chain and How It Can Protect Against Attacks*. Online. IEEE COMPUTER SOCIETY. Dostupné z: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks. [cit. 2024-01-25].

DIOGENES, Yuri a OZKAYA, Erdal, 2018. *Cybersecurity - attack and defense strategies: infrastructure security with Red Team and Blue Team tactics*. 1. Birmingham; Mumbai: Packt. ISBN 9781788475297.

GELDENHUYS, Kotie, 2021. Spyware: SPYING ON EVERYTHING YOU DO. Online. *Servamus Community-based Safety*. Roč. 114, č. 10, s. 15-18. ISSN 10152385. Dostupné z:

https://search.ebscohost.com/login.aspx?direct=true&db=asn&an=152728794&scope=site. [cit. 2023-10-22].

HADNAGY, Christopher, 2018. *Social Engineering: The Science of Human Hacking*. Second edition. Indianapolis: John Wiley & Sons. ISBN 978-1-119-43338-5.

HASHEMI-POUR, Cameron a CHAI, Wesley, 2023. *CIA triad (confidentiality, integrity and availability)*. Online. TechTarget. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [cit. 2024-01-03].

KOLOUCH, Jan, 2016. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o. ISBN 978-80-88168-18-8.

KOLOUCH, Jan; BAŠTA, Pavel; KROPÁČOVÁ, Andrea a KUNC, Martin, 2019. *CyberSecurity*. 1. Praha: CZ.NIC, z. s. p. o. ISBN 978-80-88168-31-7.

KOPÁČ, Jiří, 2023. *ESET Threat Report H2 2023*. Online. In: ESET RESEARCH. Welivesecurity. 19. 12. 2023. Dostupné z: https://www.welivesecurity.com/en/eset-research/eset-threat-report-h2-2023/. [cit. 2024-03-02].

LANGRIDGE, Marianne, 2022. *INFORMATION TECHNOLOGY FOR WATER AND WASTEWATER UTILITIES*. 2. Alexandria: Water Environment Federation. ISBN 978-1-57278-415-4.

LENAERTS-BERGMANS, Bart, 2023. *WHAT ARE COMMAND AND CONTROL (C&C) ATTACKS?* Online. CROWDSTRIKE. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/command-and-control/. [cit. 2024-01-25].

LUTKEVICH, Ben; CLARK, Casey a SHEA, Sharon, 2021. *Whaling attack (whaling phishing)*. Online. TechTarget. Dostupné z: https://www.techtarget.com/searchsecurity/definition/whaling. [cit. 2023-12-27].

MARTÍNEZ, Roberto, 2022. *Incident Response with Threat Intelligence*. 1. Birmingham: Incident Response with Threat Intelligence. ISBN 978-1-80107-295-3. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=edsknv&an=edsknv.kt0134KBT7&scope=site.

MUKESH, Kumar; NAVPREET, Kaur; SUKHJINDER, Kaur a RAJPAL, Singh, 2016. Different Security Threats and its Prevention in Computer Network. Online. *Https://www.proquest.com/docview/1860624201/EE067F2CA12B4332PQ/1?accountid=15518*. Roč. 7, č. 6, s. 87. ISSN 09765697. Dostupné z: https://www.proquest.com/docview/1860624201/EE067F2CA12B4332PQ/1?accountid=15518. [cit. 2023-10-13].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2020. *Zpráva o stavu kybernetické bezpečnosti ČR - 2019*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf. [cit. 2024-04-08].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2022. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z:

https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf. [cit. 2024-04-08].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2024-04-08].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2021. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf. [cit. 2024-04-08].

NMN NOBLES, Calvin; L BURTON, Sharon; NORMAN BURRELL, Darrell; FATAI ADEDOYIN, Festus a CHRISTIANSEN, Bryan, 2023. Cybercrime as a Sustained Business. Online. In: *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*. 1. IGI Global, s. 98-120. ISBN 9781668472095. Dostupné z: https://www.researchgate.net/publication/369973142_Cybercrime_as_a_Sustained_Business. [cit. 2023-12-29].

NOBLES, Calvin; L. BURTON, Sharon a NORMAN BURRELL, Darell, 2023. *Handbook of Research on Cybersecurity Risk in Contemporary Business*. Online. IGI Global. ISBN 9781668472101. Dostupné z: https://doi.org/10.4018/978-1-6684-7207-1.ch005. [cit. 2023-12-29].

ONDRÁK, Viktor; SEDLÁK, Petr a MAZÁLEK, Vladimír, 2013. *PROBLEMATIKA ISMS V MANAŽERSKÉ INFORMATICE*. Brno: CERM. ISBN 978-80-7204-872-4.

ROSER, Christoph, 2017. *Západní PDCA cyklus (By Christoph Roser at AllAboutLean.com under the free CC-BY-SA 4.0 license.)*. Online. In: ONDRA, Pavel. PRŮMYSLOVÉ INŽENÝRSTVÍ. Dostupné z: https://www.prumysloveinzenyrstvi.cz/2017/09/27/pdca-2-cast-historie-bezne-chyby/. [cit. 2024-01-01].

SBAI, Hugo; GOLDSMITH, Michael; MEFTALI, Samy; HAPPA, Jassim; HUTCHISON, David et al., 2018. A Survey of Keylogger and Screenlogger Attacks in the Banking Sector and Countermeasures to Them. Online. *Cyberspace Safety and Security: 10th International Symposium, CSS 2018, Amalfi, Italy, October 29–31, 2018, Proceedings*. Roč. 11161, č. 11161, s. 18-32. ISBN 9783030016883. ISSN 03029743. Dostupné z: https://doi.org/10.1007/978-3-030-01689-0_2. [cit. 2023-10-23].

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. *KYBERNETICKÁ (NE)BEZPEČNOST*. 1. Brno: CERM. ISBN 978-80-7623-068-2.

SOKOLOV, Michael, 2022. *Five years of WannaCry: what has changed in ransomware since 2017?* Online. CyberCube. Dostupné z: https://insights.cybcube.com/en/five-years-of-wannacry-ransomware?hs_amp=true&utm_term=&utm_campaign=FY22_Q4_+Brand+Awareness+/+Performance+Max+(EMEA)&utm_source=adwords&utm_medium=ppc&hsa_acc=1114695891&hsa_cam=20416089321&hsa_grp=&hsa_ad=&hsa_src=x&hsa_. [cit. 2023-09-29].

SZOR, Petr, 2006. *Počítačové viry: analýza útoku a obrana*. 1. Brno: ZONER software. ISBN 80-86815-04-8.

WICKRAMASINGHE, Shanika, 2023. *Most Common Types of Ransomware Today*. Online. Splunk. Dostupné z: https://www.splunk.com/en_us/blog/learn/ransomware-attack-types.html. [cit. 2024-04-08].

YADAV, Ajay, 2014. *Exploiting by information disclosure, part 1*. Online. INFOSEC. Dostupné z: https://resources.infosecinstitute.com/topics/application-security/exploiting-information-disclosure-part-1/. [cit. 2024-01-05].

YADAV, Tarun a MALLARI, Rao Arvind, 2015. Technical Aspects of Cyber Kill Chain. Online. *Security in Computing and Communications*. Roč. 2015, č. 536, s. 441-442. Dostupné z: https://doi.org/10.1007/978-3-319-22915-7_40. [cit. 2024-01-20].

YDAV, Tejas, 2021. *CIA AND DAD TRIAD*. Online. Medium. Dostupné z: https://medium.com/@yadavtejas249/cia-and-dad-triad-ef84a94f9aee. [cit. 2024-01-05].

ČESKO, 2023. Návrh zákona o kybernetické bezpečnosti. Online. In: . Dostupné z: https://www.zakonyprolidi.cz/media2/file/2401/File64629.pdf?attachment-filename=7704636-2023-07-19-text-navrhu-7824803.pdf. [cit. 2024-003.-14].

CYBELANGEL, 2023. *What are Infostealers?* Online. CybelAngels. Dostupné z: https://cybelangel.com/what-are-infostealers/. [cit. 2023-10-27].

MITRE, 2024. *ATT&CK Matrix for Enterprise*. Online. MITRE. MITRE|ATT&CK. Dostupné z: https://attack.mitre.org/. [cit. 2024-03-10].

ORACLE, 2024. *6.2. Introduction to Networking Modes*. Online. ORACLE. VirtualBox. Dostupné z: https://www.virtualbox.org/manual/ch06.html#network_vde. [cit. 2024-03-07].

Servamus Community-based Safety & Security Magazine, 2021. NSO Group Technologies (Company). ISSN 1015-2385.

MANSDORF S. Z., 2019. *Handbook of Occupational Safety and Health (3rd Edition)*. ISBN 9781523128211. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=edsknv&an=edsknv.kt0125ESX2&scope=site.

ČESKO, 2009. Zákon č. 40/2009 Sb. Zákon trestní zákoník. In: . Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40?text=40%2F2009. [cit. 2024-01-28].

ČESKO, 2014. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti): Zákon o kybernetické bezpečnosti. Online. In: . Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181?text=181%2F2014. [cit. 2024-003.-13].

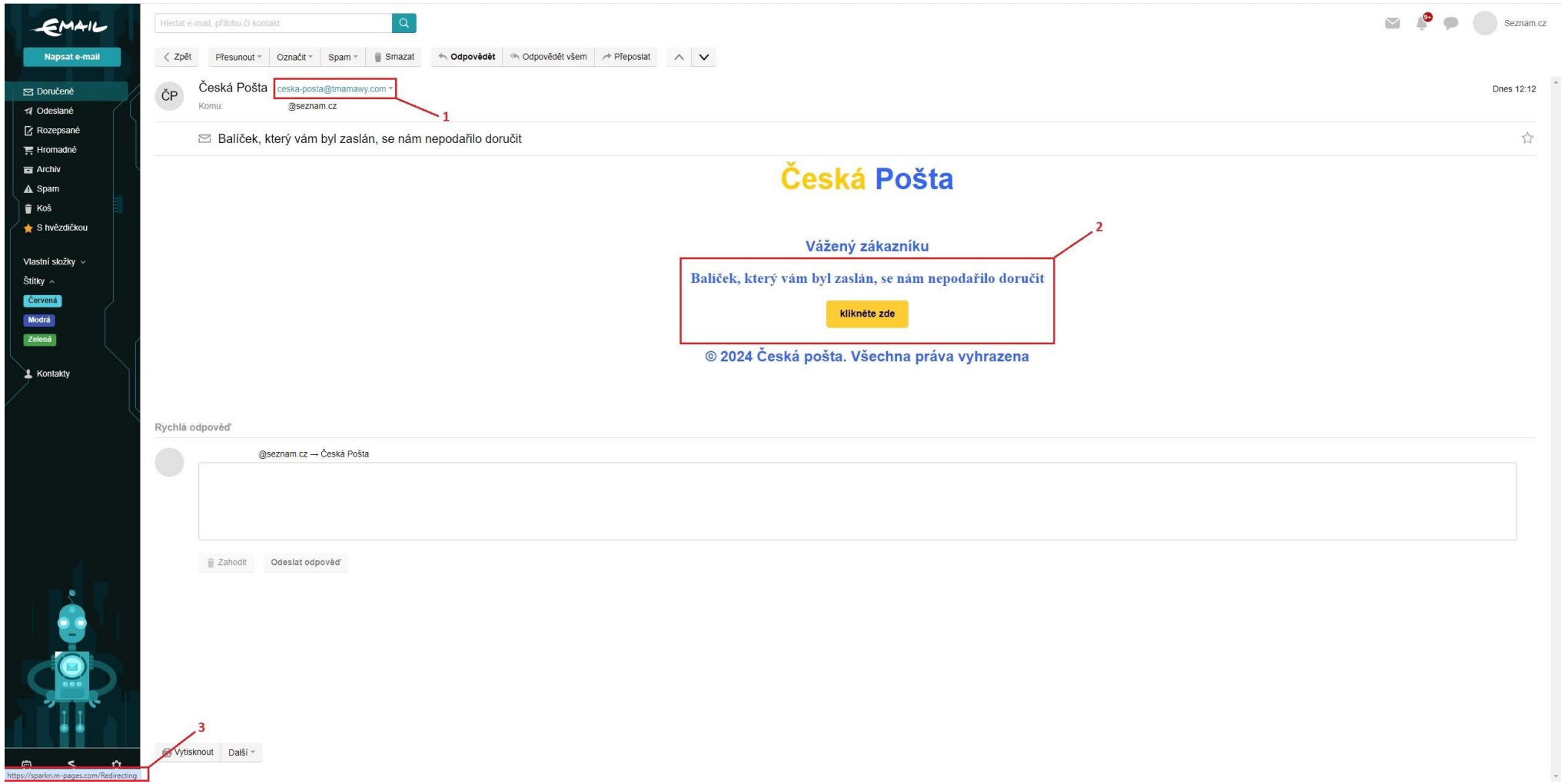
SECUREWORKS, 2017. *WCRY RANSOMWARE ANALYSIS*. Online. Secureworks. Dostupné z: https://www.secureworks.com/research/wcry-ransomware-analysis. [cit. 2024-01-05].

SEZNAM OBRÁZKŮ

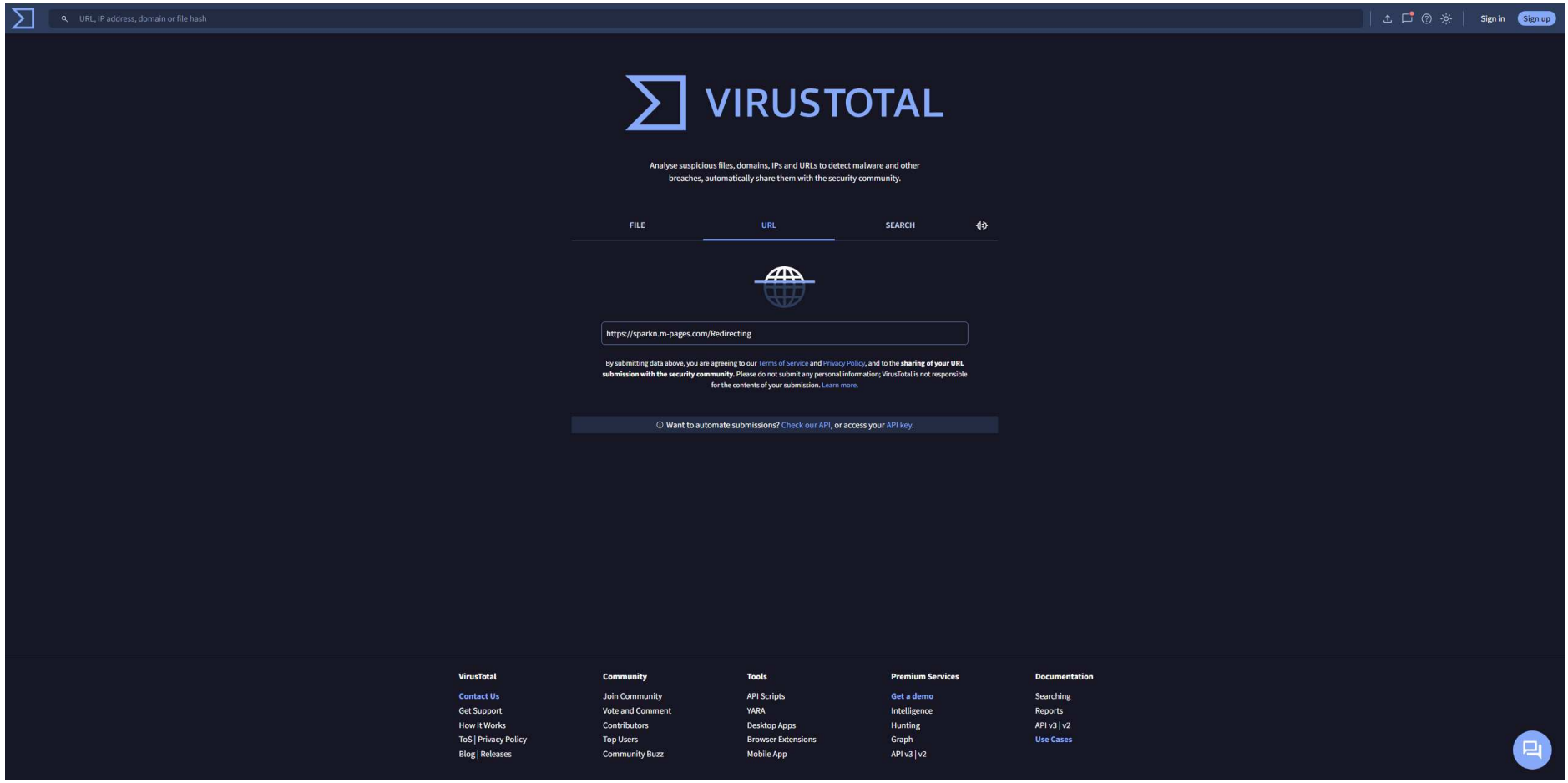
SEZNAM TABULEK

SEZNAM PŘÍLOH

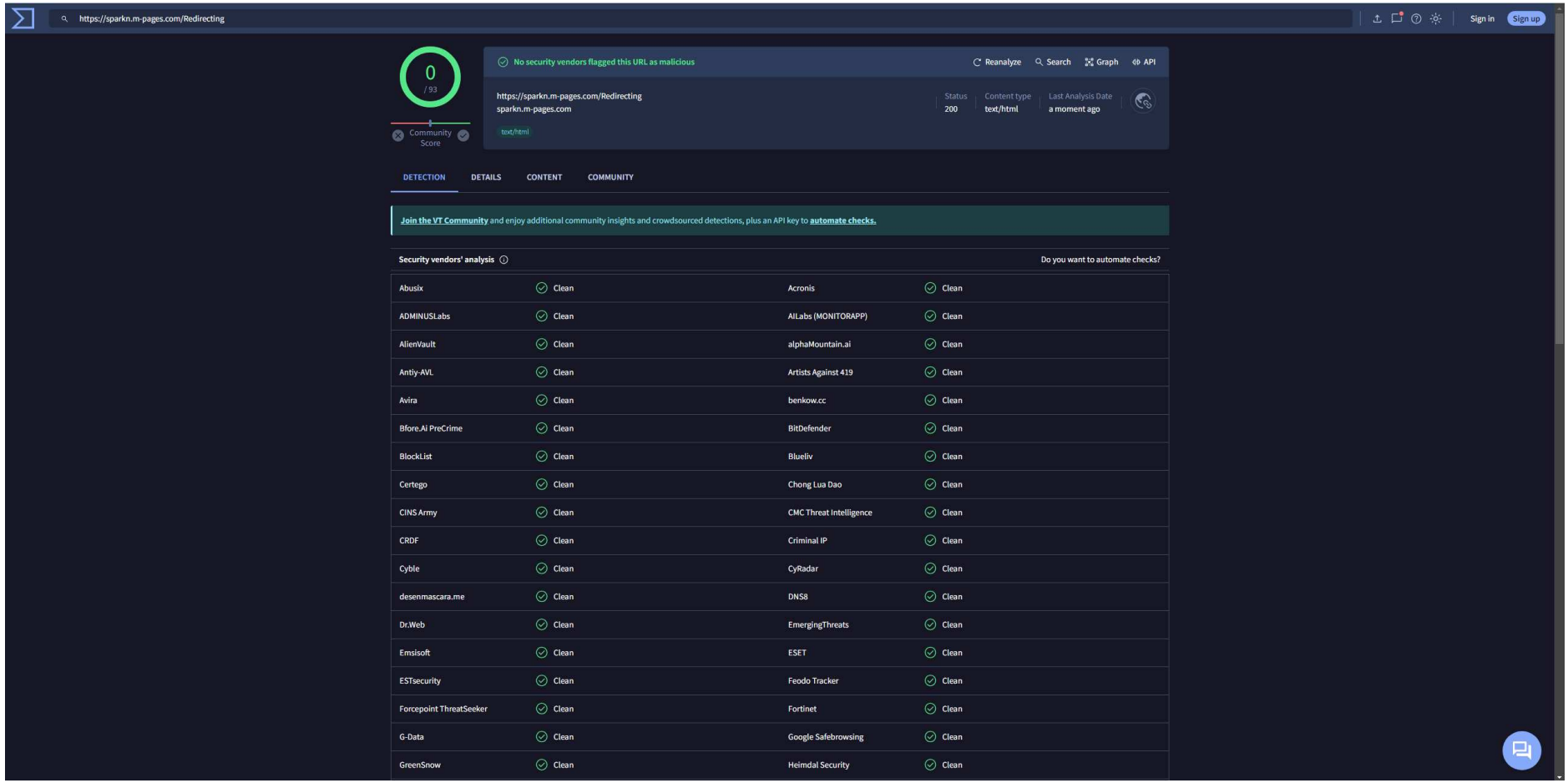
PŘÍLOHA P I: PODVODNÝ EMAIL OD ČESKÉ POŠTY



PŘÍLOHA P II: OVĚŘENÍ URL ADRESY POMOCÍ NÁSTROJE VIRUSTOTAL



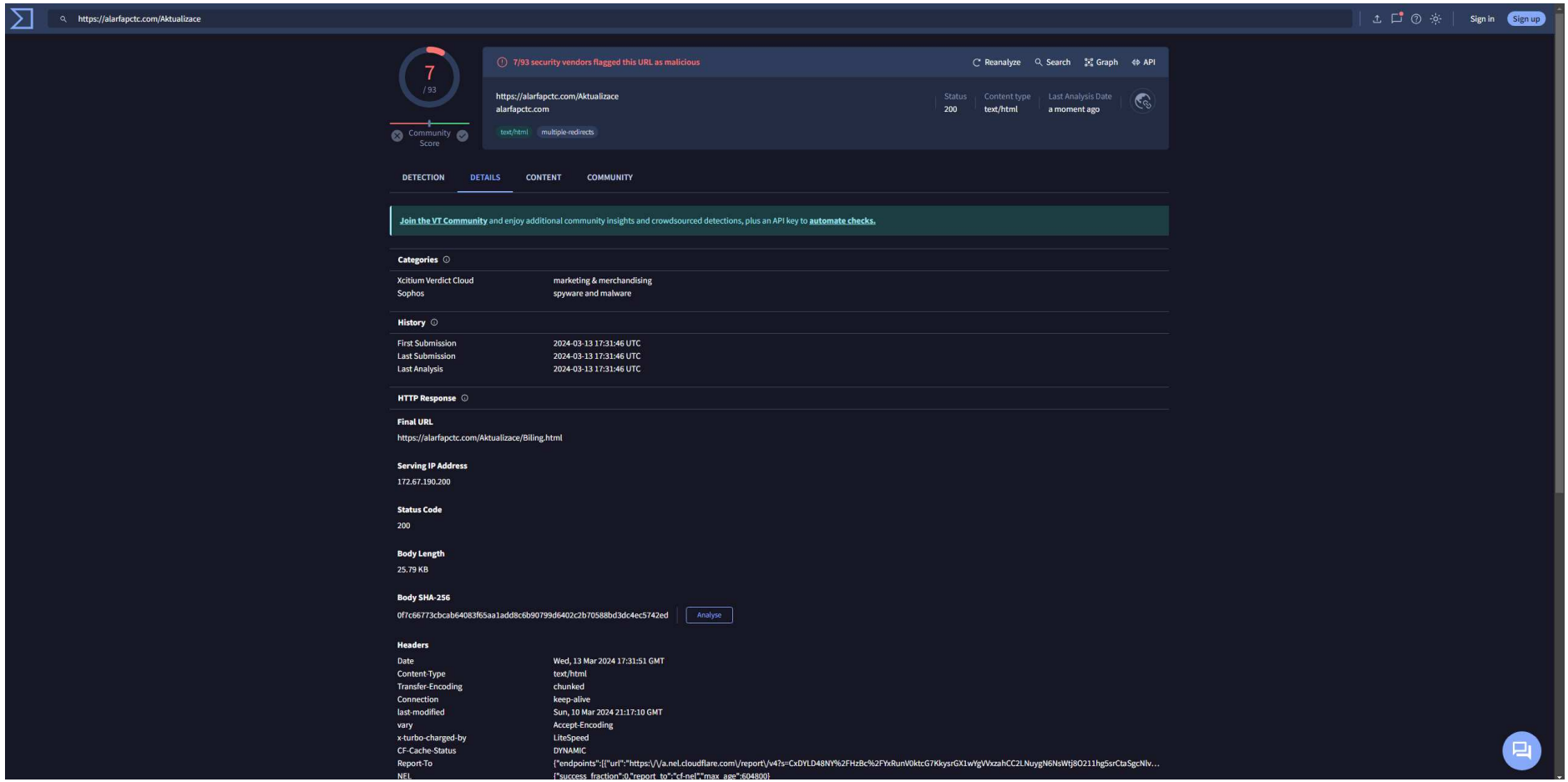
PŘÍLOHA P III: VÝSLEDEK PRVNÍHO SKENU URL ADRESY



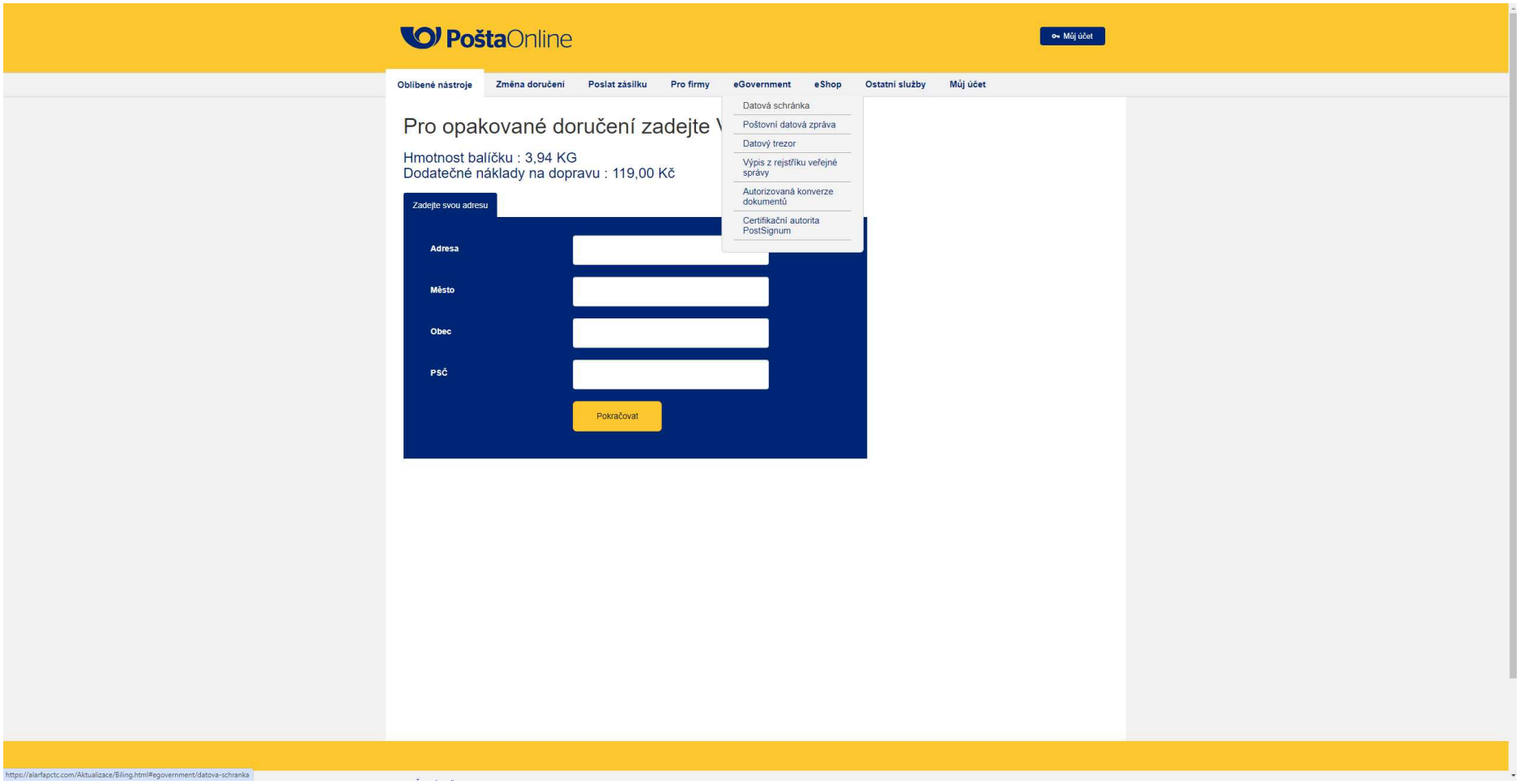
PŘÍLOHA P IV: PRVNÍ STRÁNKA PO PŘESMĚROVÁNÍ

https://alarfapctc.com/Aktualizace

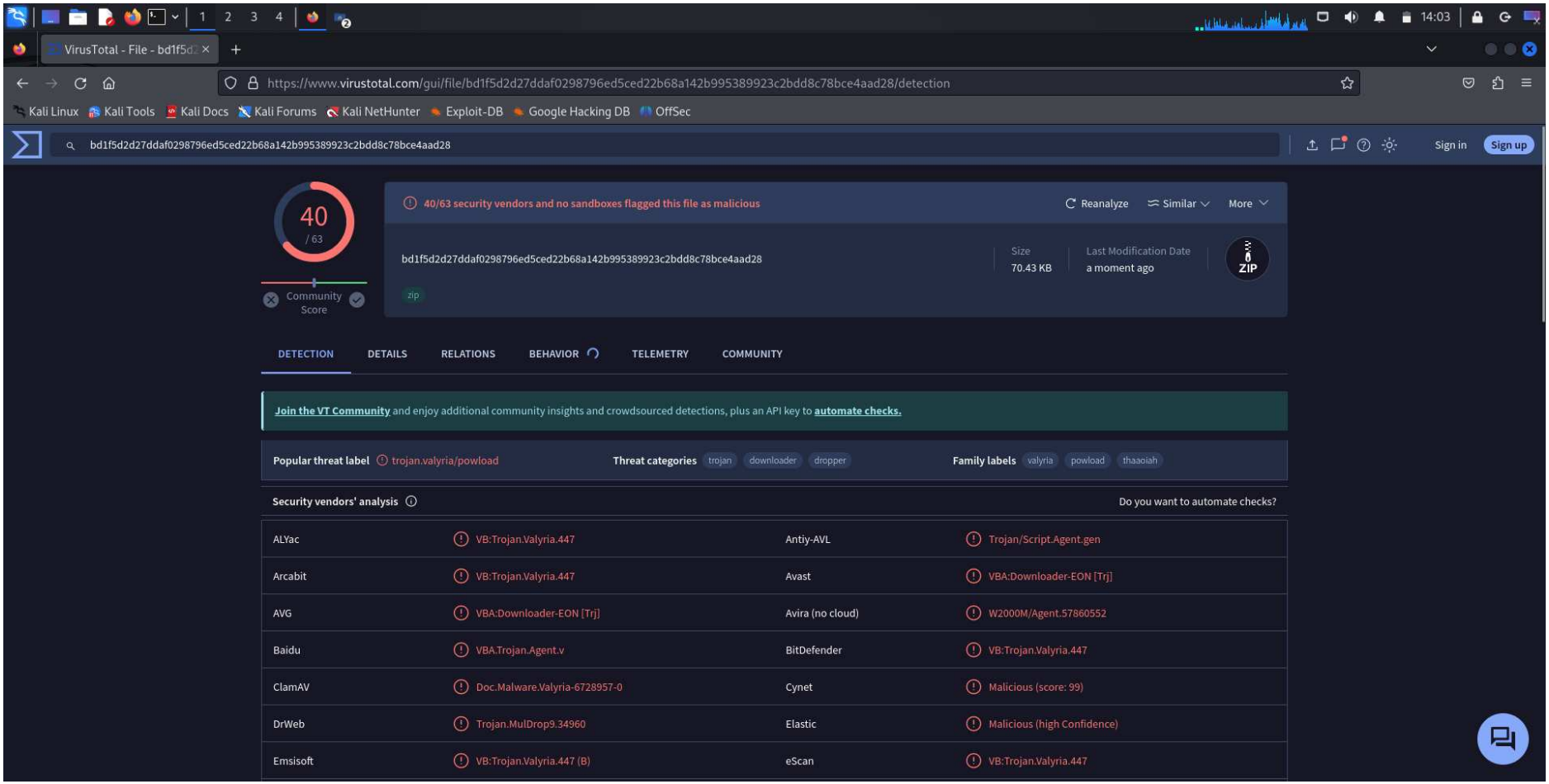
PŘÍLOHA P V: VÝSLEDEK SKENU DRUHÉHO ODKAZU



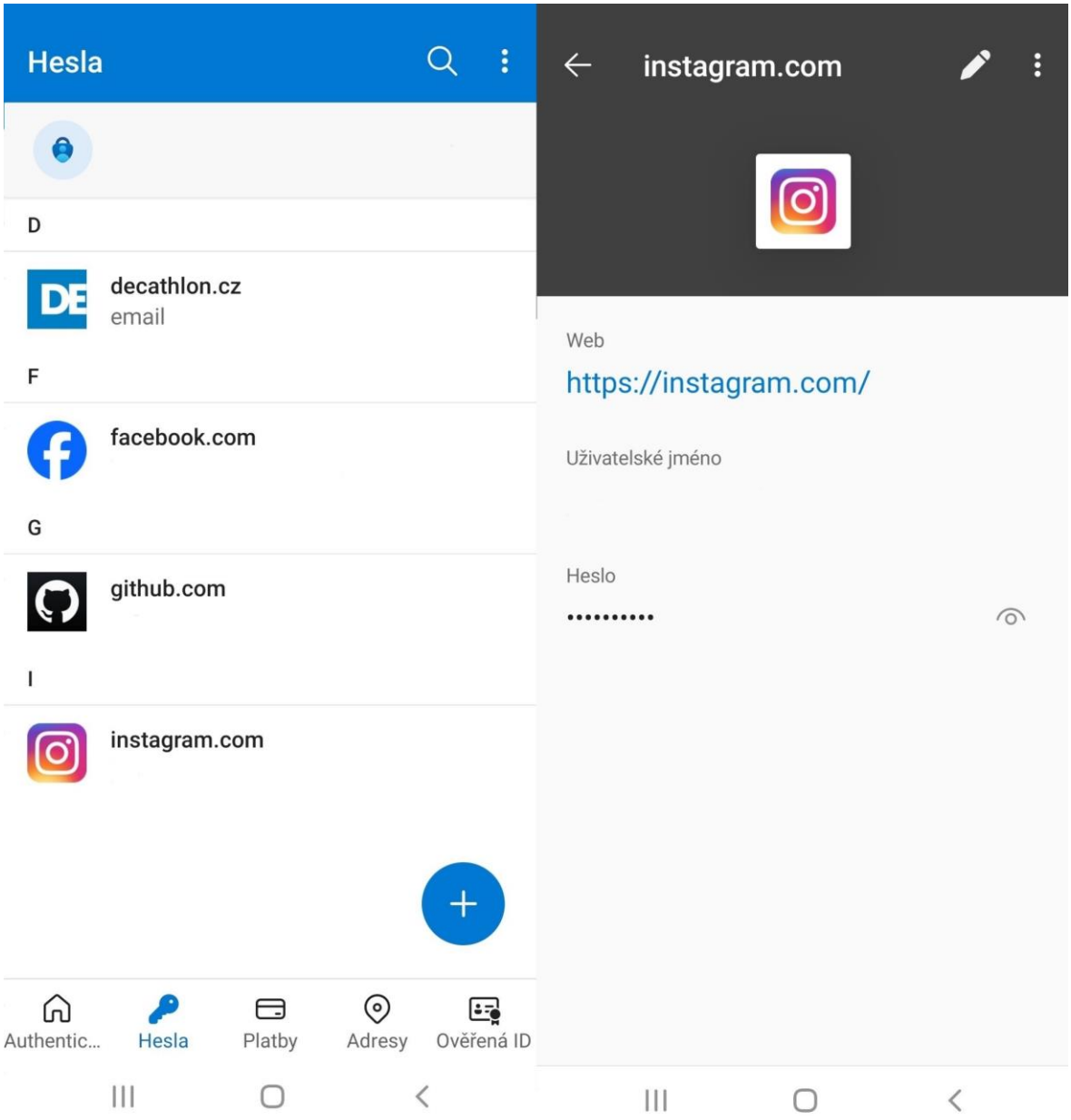
PŘÍLOHA P VI: PODVODNÝ PORTÁL ČESKÉ POŠTY



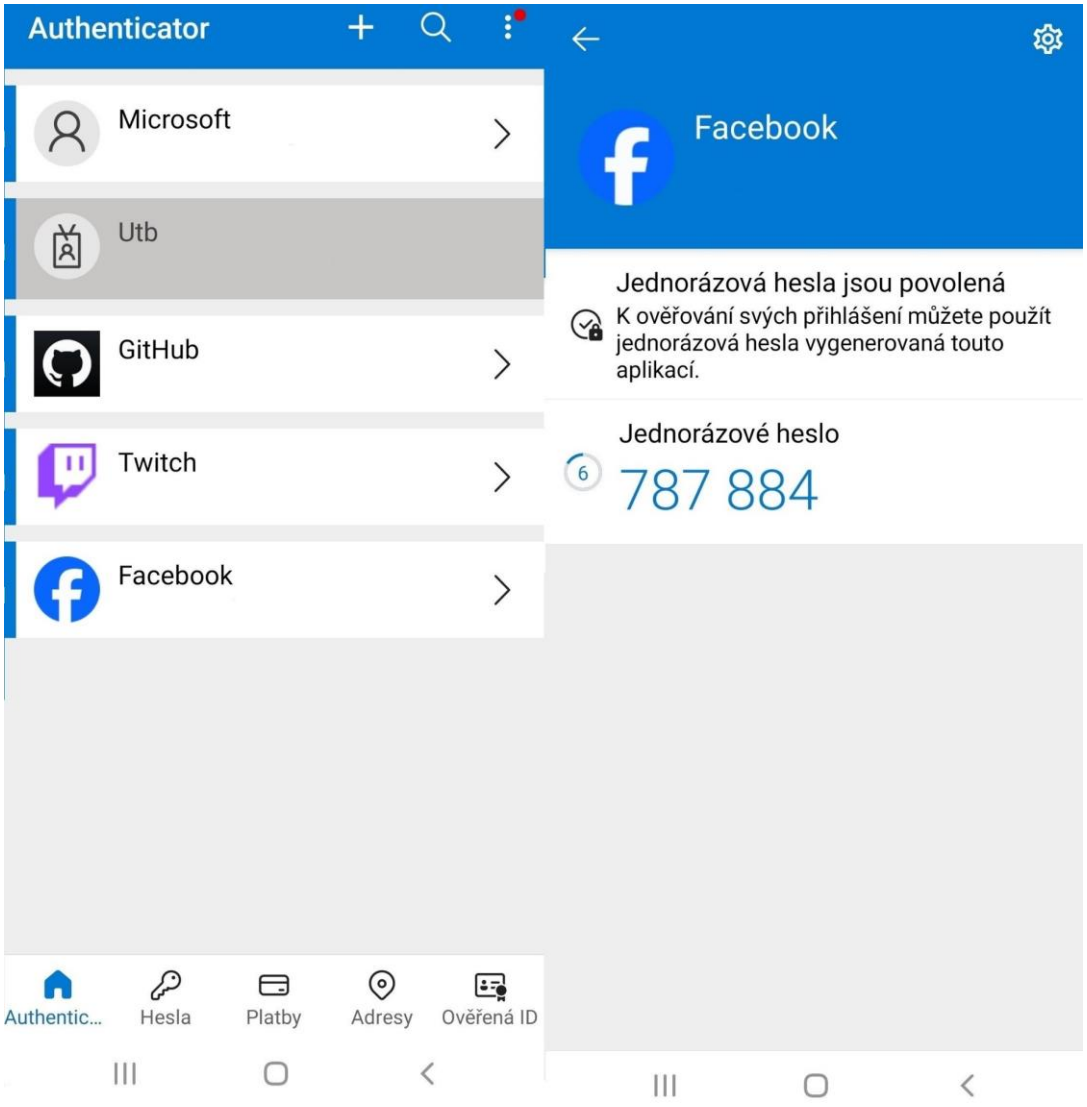
PŘÍLOHA P VII: VÝSLEDEK SKENU PŘÍLOHY POUŽITÉ VE SCÉNÁŘI



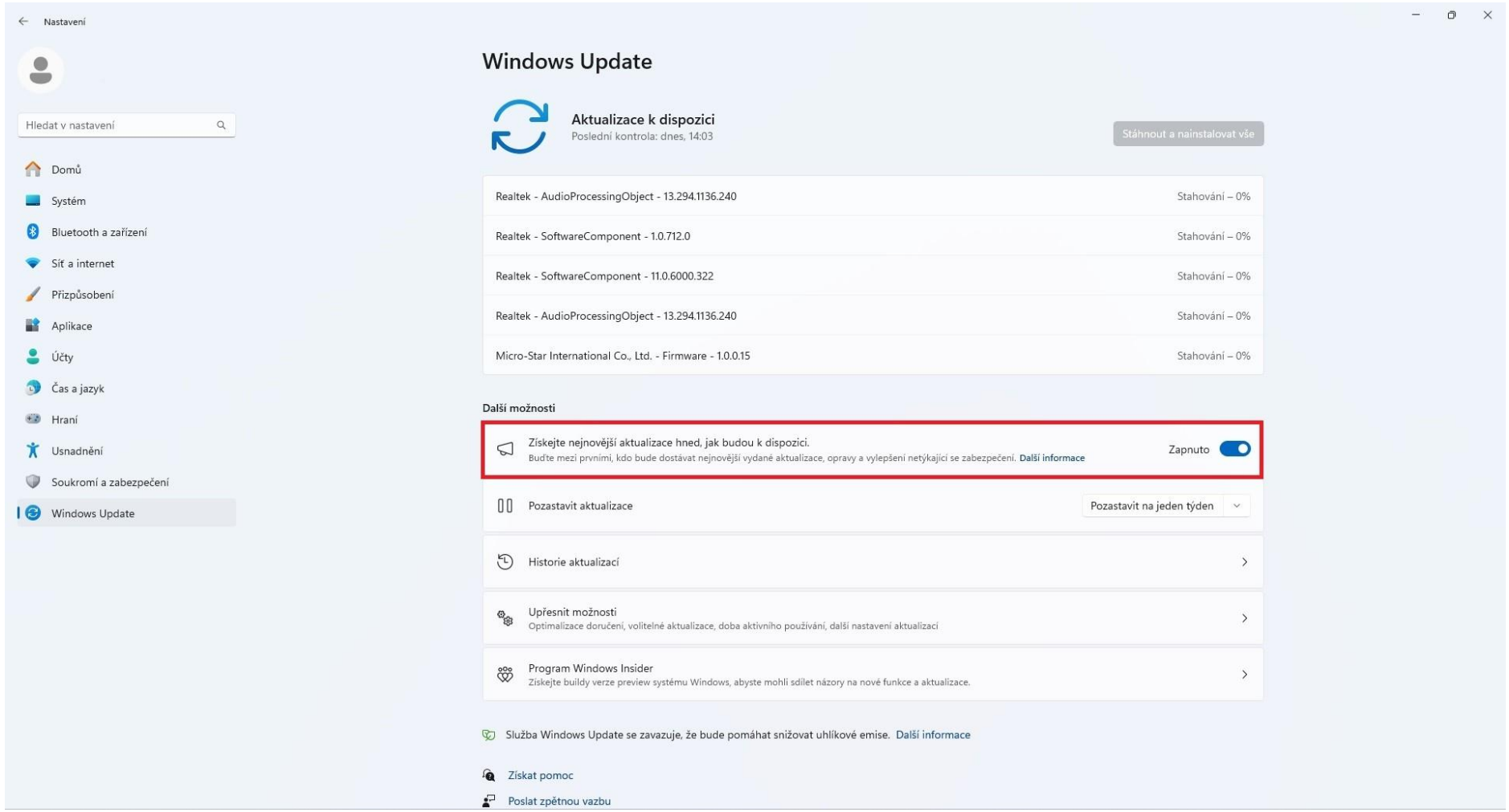
PŘÍLOHA P VIII: SPRÁVCE HESEL



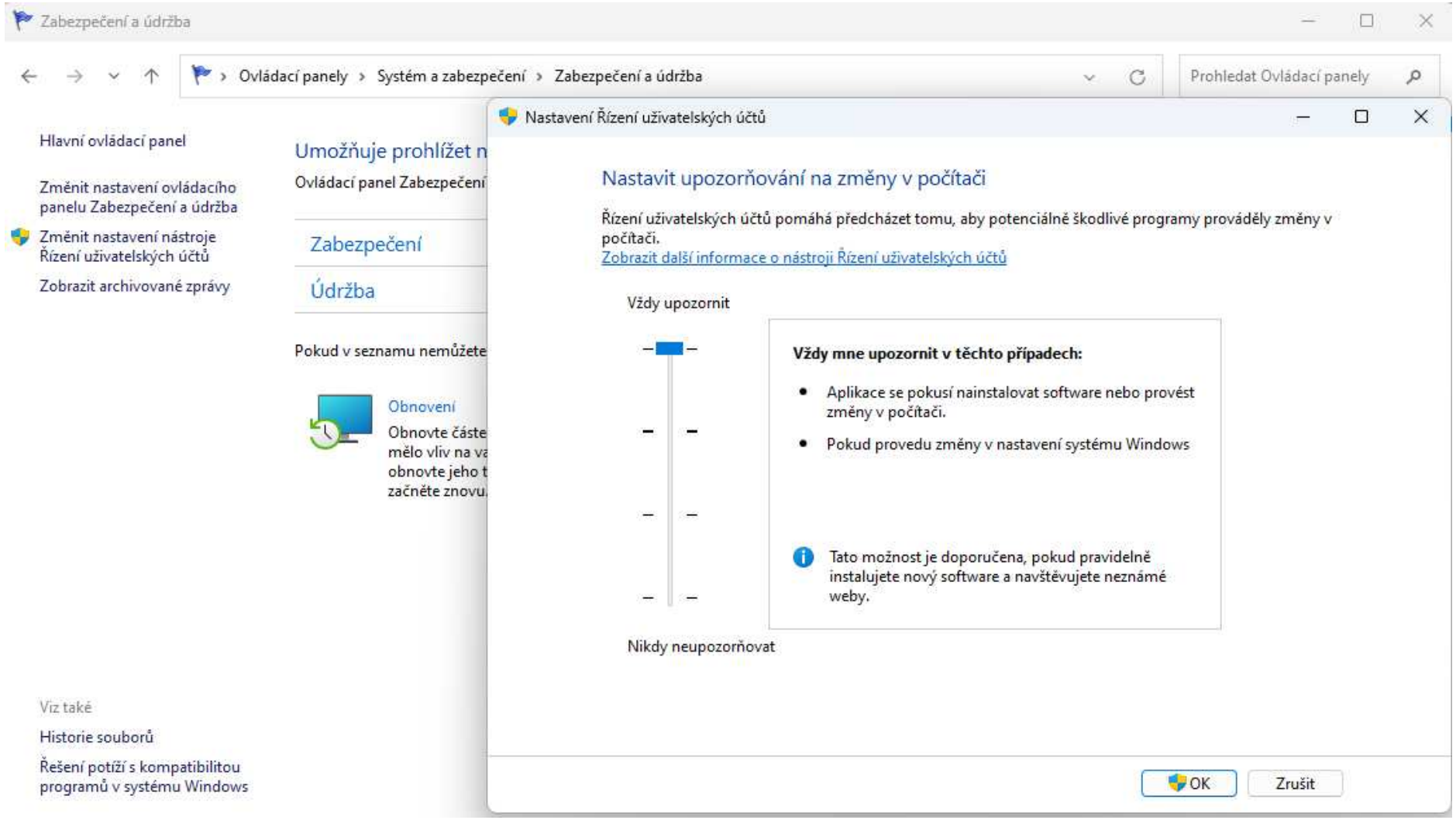
PŘÍLOHA P IX: APLIKACE PRO VÍCEFAKTOROVÉ OVĚŘENÍ



PŘÍLOHA P X: NASTAVENÍ AKTUALIZACÍ V SYSTÉMU WINDOWS



PŘÍLOHA P XI: NASTAVENÍ ŘÍZENÍ UŽIVATELSKÝCH ÚČTŮ (UAC)



PŘÍLOHA P XII: MOŽNOSTI KONTROLY SYSTÉMU POMOCÍ MICROSOFT DEFENDER