Kategorizácia veľkého množstva spamových e-mailov

Tomáš Spevák

Bakalárska práca
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš Spevák**
Osobní číslo:	**A16069**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Kategorizace velkého množství spamových e-mailů**
Téma anglicky:	**The Categorisation of a Large Number of Spam E-Mails**

Zásady pro vypracování:

1. **Nastudujte terminologie a popište základní rozdíly v rámci spamových e-mailů.**
2. **Navrhněte způsob pro hromadnou analýzu a klasifikaci velkého množství nevyžádané elektronické pošty.**
3. **Vytvořte skripty pro získání a kategorizaci informací z balíku spamových e-mailů.**
4. **Proveďte klasifikaci a samotnou analýzu získaných dat.**
5. **Vhodně reprezentujte a popište výsledky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BRUNTON, Finn. Spam: a shadow history of the Internet. Cambridge, Massachusetts: The MIT Press, 2013. Infrastructures. ISBN 978-0-262-31394-0.
2. AKERLOF, George A a Robert J SHILLER. Jak se loví hlupáci: ekonomie manipulace a klamu : nenechte sebou manipulovat. Praha: Management Press, 2017, 264 s. ISBN 978-80-7261-478-3.
3. XIAO, Yang, Frank H. Li, Hui ChenHandbook of Security and Networks [online]. [cit. 2018-11-26]. ISBN 978-981-4468-03-9.
4. MERHAUT, Filip a Ivan ZELINKA. Počítačové viry a bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008 [i.e. 2009], 142 s. ISBN 978-80-7318-763-7.
5. JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.
6. SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 80-86815-04-8.
7. JONES, Dennis. Jak využívat Internet. Praha: SoftPress, c2001, 398 s. ISBN 80-86497-12-7.

Vedoucí bakalářské práce: **Ing. Petr Žáček**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **21. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 21. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13.5.2019

Tomáš Sperák, v.r.
podpis diplomanta

ABSTRAKT

Cieľom tejto práce je priblížiť čitateľom problematiku spamových emailov a popísať jednotlivé rozdiely v rámci spamových emailov, navrhnúť a vytvoriť skripty pre triedenie týchto spamových emailov za účelom štatistiky, z ktorej je možné zistiť dôležité informácie ako odkiaľ emaily pochádzajú, počet krajín zapojených do odosielania alebo či tieto emaily majú vydieračský charakter. Ďalšia časť je o virtuálnej mene bitcoin, ktorá je často využívaná práve na transakcie spojené s vydieračskými emailmi, pričom sumy, ktoré sú z nich získané, sú uložené v bitcoinových peňaženkách útočníkov.

Kľúčové slová: emailová správa, spam, phishing, scam, bitcoin

ABSTRACT

The main purpose of this work is to introduce the public to the issue of spam and describe the differences between spam emails, to plan and to create the scripts to sort these spam emails for statistics, from which it is possible to find out important informations like from where the emails come from, how many countries are involved into sending these emails or to find out if they have blackmailing character. Next part is about virtual currency bitcoin, which is often used for transactions connected to these blackmailing emails, while the gathered amounts are stored in bitcoin wallets of attackers.

Keywords: email message, spam, phishing, scam, bitcoin

Touto cestou by som rád poďakoval svojmu vedúcemu práce Ing. Petru Žáčkovi za pomoc, ktorú mi poskytol pri vytváraní bakalárskej práce, za ochotu venovať mi plne svoj čas počas konzultačných hodín a za vedenie celej práce.

Taktiež by som chcel poďakovať svojej rodine, ktorá ma vo všetkom podporovala a umožnila mi štúdium na vysokej škole.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Jednoduché a laické vysvetlenie, čo spam je, ponúka stránka Zoznam: „*E-mailový spam je nevyžiadaná e-mailová správa, často s komerčným obsahom, doručovaná veľkým množstvám príjemcov.“* [1] Práca sa zaoberá jednou z najdôležitejších tém internetu a komunikácie. Jedná sa o nevyžiadanú poštu, taktiež nazývanú spam, ktorá sa denne rozposiela miliónom užívateľov v enormných množstvách po celom svete. Nakoľko existuje veľa druhov spamu, nie je ho ľahké jednoznačne zadefinovať, keďže každý si môže pod týmto pojmom predstaviť niečo úplne iné.

Túto prácu som si vybral preto, že téma spam ma zaujala vzhľadom k tomu, že sa jedná o jeden z najväčších problémov súčasnosti, čo sa internetovej komunikácie týka. Cieľom práce je popísať rôzne typy nevyžiadanej pošty, uviesť príklady a následne vykonať kategorizáciu tejto nevyžiadanej pošty. Zameriavam sa hlavne na zistenie údajov ako napr. odkiaľ spamové emaily prichádzajú, koľko ich priemerne pochádza z jednej adresy, a či niektoré z emailov majú vydieračský obsah a charakter. Snažím sa o to, aby si bežný užívateľ mohol vytvoriť obraz o tom, aký veľký je tento problém nevyžiadanej pošty, a aby mal prehľad, z ktorých krajín je táto pošta najčastejšie odosielaná, prípadne či si treba dávať pozor na výskyt nejakého vírusu alebo vydieračského obsahu. Pre prácu sú preto vytvorené skripty, ktoré analyzujú veľké množstvo nevyžiadanej pošty a zisťujú z neho dôležité informácie, ako napr. IP adresu, krajinu, prílohu, či email obsahuje odkaz na nejakú stránku a pod.

V prvej časti práce vysvetľujem terminológiu, ktorá sa týka spamových emailov, teda napr. čo je to spam, akú má históriu, či existuje protiklad spamu, čo je to pharming a phishing, popisujem menu bitcoin, ktorá sa využíva pri vydieračských útokoch a pod. V druhej kapitole vytváram návrh, pomocou ktorého som zrealizoval skripty pre klasifikáciu týchto emailov. V tretej časti sú popísané vytvorené skripty v programovacom jazyku Python, ktorých výstupom bude .csv súbor, v ktorom sú zapísané všetky údaje, ktoré bolo možné analýzou zistiť. Vo štvrtej kapitole sa ďalej venujem spracovaniu tohto výstupu do grafov. Grafy budú prehľadom toho, odkiaľ tieto emaily a spameri, teda osoby rozosielajúce tento druh pošty pochádzajú, a či sa k emailu viaže aj nejaký súbor ako príloha. Piata časť je celá venovaná problematike vydieračských emailov, priblíženiu presnejšieho popisu týchto emailov, teda v akom jazyku boli písané najčastejšie, koľko jazykov v nich bolo použitých, aké sumy a v akých menách útočníci žiadali, a taktiež kam peniaze smerovali, a koľko sa ich

približne od potenciálnych obetí podarilo získať. Posledná šiesta časť je venovaná zhrnutiu údajov, ktoré bolo možné zistiť z poskytnutého balíku.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÉ ROZDIELY V RÁMCI SPAMOVÝCH EMAILOV

Oblasť spamových emailov je natoľko komplexná, že je potrebné popísať jej základné rozdiely pre lepšie odlíšenie jednotlivých kategórii spamových emailov. Tieto rozdiely budú definované v jednotlivých podkapitolách, pričom každá bude venovaná práve jednej kategórii.

1.1 Spam

Spam v počítačovej technike značí niečo nechcené. Samotné slovo spam väčšinou odkazuje na nechcenú správu alebo nechcený email, vo väčšine prípadov sa môže jednať o ponúkanie nejakého tovaru, popr. cielenú reklamu na určité služby. Taktiež sa označuje ako Unsolicited Bulk Email (UBE), v preklade nežiadaný hromadný email, popr. je tiež označovaný ako Unsolicited Commercial Email (UCE), teda nežiadaný komerčný email. Spam je tiež často označovaný ako odpad. V najväčšej časti tvoria spamové emaily komerčné ponuky, reklamy na tovar alebo službu, občas sa ale jedná aj o emaily s úmyslom uškodiť (phishing, pharming). Samotné spamové emaily vo veľkej časti vylučujú emaily zo známych zdrojov, viac-menej sa zvykne jednať o pochybných odosielateľov, aj keď obsah samotného emailu môže byť známy. Malware a vírusy ako také sa normálne nezaraďujú ako spamový email, aj keď niektoré vlastnosti s nimi zdieľajú. [1,2]

Ľudia, ktorých prácou je rozosielanie takýchto spamových emailov sú spameri. Spoločnosti ich zväčša zamestnávajú, pretože odosielaním takýchto emailov zvýšia popularitu svojho produktu. Spameri samotní k tomu využívajú svoje vlastne navrhnuté algoritmy a programy, popr. technológie, ktoré boli vyvinuté špeciálne na hromadné rozosielanie tejto nežiadanej pošty. Existujú však aj určité programy a antispamové nástroje, ktoré spamy blokujú a neumožnia im prejsť až do emailovej schránky. [1]

1.1.1 História spamu

Meno tohto nežiadaného emailu pochádza zo známeho mäsa v konzerve, ktoré nesie rovnaký názov. Nápad, že by tieto nevyžiadané emaily mohli niesť rovnaký názov, prišiel vtedy, keď skupina komediantov Monty Python vytvorila na toto jedlo pieseň nazývanú „*Spam Song*“. V tejto piesni skupina Vikingov spieva dookola slovo spam, zakaždým so zvyšujúcou sa hlasitosťou, až to začne byť nežiadané a Vikingovia musia byť umlčaní. Od

tej doby sa začalo slovo spam používať aj pre pomenovanie niečoho, čo sa neustále opakuje tak veľmi, až to obťažuje, popr. to je nechcené. [2]

Prvý email na svete bol poslaný v roku 1971, pričom prvý spamový email prišiel pár rokov na to, konkrétne 3.5.1978. Vtedy americká vláda financovala Arpanet. Prvý spamer bol Gary Thuerk, ktorý pracoval v spoločnosti DEC. Obsah emailu bola číra reklama na novú verziu operačného systému práve pre počítače od DEC a na podporu pre prácu v sieti Arpanet. Gary Thuerk týmto emailom taktiež všetkých príjemcov pozval na prezentáciu nových produktov. Keďže bol email odoslaný používaním Arpanetu, odpoveď od jej riaditeľa bola takmer okamžitá, a ten toto chovanie vzal ako porušenie obchodných podmienok siete Arpanet. [3]

Spam sa vo väčších množstvách začal rozosielať až roku 1994, kedy Laurence Carter, právnik z Arizony, automatizoval rozosielanie správ na veľké množstvo internetových skupín, čím chcel dosiahnuť zviditeľnenie služieb jeho firmy. Výsledkom tohto činu bolo sťažovanie sa používateľov siete Usenet, ktorí takéto správy označili za „spam“. Týmto sa začalo hromadné rozosielanie spamových emailov tak, ako je to známe dnes. [3]

Od týchto čias sa počet spamových emailov len a len zvyšoval. Podľa štatistík zo svetoznámej stránky Statista sa denne pošle takmer 300 miliárd emailov, z nich 54% tvorí spam. V druhom štvrťroku roku 2018 viedla v rozosielaní spamových emailov Čína, ktorá poslala 14.36% spamových emailov. [4]

1.1.2 Antispamové techniky

Spam je každým rokom stále väčším problémom, pričom metódy doručovania spamu sú rok čo rok sofistikovanejšie. Tomu sa musia prispôsobovať aj antispamové techniky, ktorých úloha je blokovať takéto emaily v závislosti od kľúčových slov, ktoré sa v nich nachádzajú, cez blacklisty adries z ktorých emaily prichádzajú. Metódy antispamových techník sú napr.:

- **Filter slov**
    - Existujú rôzne databázy slov, v ktorých sú uložené práve kľúčové slová, podľa ktorých má byť správa filtrovaná. Príkladom takýchto kľúčových slov môžu byť napr. výrazy ako „predaj“, „kúp“, alebo tiež slovné spojenie „posledná šanca“ a pod. Tieto filtre sú stále vylepšované, a to tak, že do databázy sú stále pridávané nové slová, ktoré slúžia pre lepšie rozpoznanie spamu. [5]

- **Blacklisty**
    - Existujú listy a zoznamy adries, ktoré obsahujú obrovské množstvá IP adries, ktoré sú v prípade prichádzajúceho emailu skontrolované, či sa nenachádzajú práve v takomto liste. Táto antispamová technika adresu skontroluje, a v prípade, že sa v takomto liste nachádza, do emailovej schránky sa nedostane, popr. skončí v záložke spam. Ak by sa táto adresa v tomto liste nenachádzala, objaví sa priamo medzi novými správami. Rôzne druhy softvér môžu využívať aj väčší počet takýchto čiernych zoznamov, jeden program teda môže využívať aj niekoľko desiatok databáz blacklistov. [5]
- **Štatistické filtre**
    - Tieto filtre sú navrhnuté tak, aby sa postupom času učili nové, bežné slová a následne ich rozpoznávali a triedili do dvoch skupín, konkrétne spam a ham. V prípade, že by sa jednalo o spam, skončí takáto správa v nevyžiadanej pošte. Ak by sa jednalo o ham, email pokračuje ďalej do emailovej schránky. Tieto filtre fungujú na matematickej teórii, ktorá sa nazýva Bayesova analýza. Tým, ako cez tieto filtre prechádzajú nové a rôzne emaily, či už zo spam alebo ham kategórie, sa učia nové slová a rozpoznávanie je presnejšie, teda je väčšia pravdepodobnosť úspešného rozpoznania. [5]
- **Analýza hlavičky emailu**
    - Softvér využívaný spamermi často generuje hlavičky, ktoré môžu byť úplne nezmyselné alebo nezvyčajné. Táto antispamová technika tieto hlavičky kontroluje a tým oddeľuje spam od hamu. Softvér takto môže na hlavičku použiť viac testov. [5]
- **Whitelist**
    - Whitelisty sú opak blacklistov. Tak ako existuje čierna listina odosielateľov, existuje aj biela listina, do ktorej patria odosielatelia odosielajúci veľké množstvo pošty, sú ale dôveryhodní a známi, preto email od nich nebude považovaný na spam, ale ham. Nezáleží na tom, aký obsah email má, pretože automaticky bude označený ako ham a v spame neskončí. [5]

1.2 Ham alebo spam?

Najjednoduchšie je možné definovať ham nasledovne: „*Je to email, ktorý je všeobecne žiadaný a nie je považovaný za spam*.“. [6]

Môže sa stať, že v poštovej schránke skončí email, ktorý vypadá ako spam, ale nebol tak označený. Naopak email, ktorý je žiadaný, a na ktorý môže užívateľ čakať, popr. email, ktorý spamom nie je práve kvôli antispamovému filtru skončí v kategórii spamových emailov. To môže viesť k zmazaniu dôležitého emailu po uplynutí časového limitu pre ponechanie spamového emailu v poštovej schránke, čím užívateľ o tento email nenávratne príde. [6]

Keďže je ham všeobecne žiadaný, mohla by byť položená otázka, prečo email, ktorý sa javí ako spam, za spam označený nie je. Odpoveďou na túto otázku môže byť to, že aj keď si užívateľ neprial dostať takýto email, svojou nepozornosťou alebo nešikovnosťou mohol sám o takýto email, popr. väčšie množstvo emailov požiadať, a to tak, že sa prihlásil na odber takýchto emailov. Existuje niekoľko možností, akými je možné sa na takýto odber emailov prihlásiť:

- Priamo – Pri sťahovaní nejakého programu z internetu, registrácii na stránku nejakej služby, napr. obchodu pri nákupe cez e-shop, alebo pri sťahovaní nejakej internetovej hry a pod. Pri inštalácii akéhokoľvek druhu softwaru, popr. pri registrovaní sa na diskusné fórum alebo inú stránku je potrebné vyjadriť súhlas s podmienkami spoločnosti. Vo veľkom množstve prípadov sa taktiež objaví možnosť registrácie na odber novín alebo článkov od tejto stránky, služby alebo od ich partnerov. Úmyselne, ale aj omylom môže užívateľ túto možnosť potvrdiť, čím spoločnosti dá priamo súhlas s posielaním takýchto reklamných, popr. iných emailov na jeho emailovú adresu. [6]
- Nepriamo – Viac-menej sa jedná o rovnaký princíp súhlasu s odberom ako u metódy priamej, rozdiel je ale v tom, že možnosť rozhodnutia o odosielaní týchto emailov je vydavateľom softwaru, popr. tvorcom internetovej stránky predom označená. Jedinou možnosťou vyhnutia sa odberu takýchto emailov je zrušenie súhlasu užívateľa o odosielaní. [6]

Či už sa užívateľ na odber noviniek rozhodol prihlásiť priamou alebo nepriamou metódou, nevedomky alebo úmyselne, pripísal sa na hromadný zoznam emailov. Tým, že sa na tomto zozname vyskytuje, je docielené to, že odosielateľ môže plne legálne odoslať na adresu

užívateľa či už žiadanú alebo nežiadanú poštu. Existujú však isté regulácie, ktoré umožňujú sa z odberu noviniek odhlásiť. V prípade, že sú smernice dodržané, by mali prestať tieto emaily putovať na emailovú adresu. Môže sa však stať, že tieto emaily sú poslané osobou, ktorá má nečestné úmysly a využije výhodu toho, že sa chce užívateľ z odberu noviniek odhlásiť. Do odkazu, ktorý by po otvorení mal zrušiť odber noviniek infiltruje svoj vlastne navrhnutý škodlivý softvér, popr. sa začne sledovanie cookies a pod. Nestáva sa to však príliš často, naviac sa dá overiť, či odkaz skutočne vedie na stránku zrušenia odberu alebo na falošnú stránku, ktorej by sa normálne bežný užívateľ chcel vyhnúť. V prípade, že by sa pod odkazom schovával nejaký škodlivý kód, popr. iný softvér sa užívateľ stáva obeťou scamu, presnejšie pharmingu. [6]

1.3 Hoax

„*Hoax je klamstvo zámerne zhotovené tak, aby sa vydávalo za pravdu*“. [7]

Pod pojmom hoax sa najčastejšie skrýva falošná alebo poplašná správa, popr. novinárska kačica, výmysel alebo jednoducho žart. V počítačovom svete sa užívateľ môže s týmto pojmom stretnúť najčastejšie vtedy, keď sa jedná o falošnú správu, ktorá užívateľa varuje o tom, že v jeho systéme sa ukrýva nejaká skrytá hrozba. V správe môže byť napísané napr. to, že sa v počítači nachádza nejaký škodlivý kód, vírus, popr. iný malvér a je potrebné stiahnuť antivírusový program, ktorý by tento problém vyriešil. V správe môže byť takýto antivírusový program priložený, popr. je poskytnutý odkaz na jeho stiahnutie. Skutočnosť je však taká, že v počítači sa žiadny škodlivý kód ani vírus nenachádza, užívateľ si však pre istotu môže antivírusový program nainštalovať v prípade, že ho nemá. [7, 8]

Takýto druh správy sa užívateľov často snaží presvedčiť o svojej dôležitosti a väčšinou je priložený aj dôveryhodný zdroj, aby tomu užívateľ ľahšie uveril. Môže sa stať, že užívateľ obdrží email, v ktorom je varovaný napr. FBI pred novým nebezpečenstvom, ktoré sa vo svete vyskytlo, popr. pred nejakou inou nezmyselnou vecou. Dôvod, prečo užívateľ takýto email dostane je ten, že odosielateľ chce v príjemcovi vzbudiť strach či záujem. Môže sa tiež jednať o zdieľanie extrémne dôležitej a tajnej správy zo sociálnej siete, ktorú autor objavil, no médiá o nej mlčia. Vedie to väčšinou až k tomu, že autor tejto správy vyzýva ľudí k zdieľaniu tejto správy, či už na sociálnych sieťach alebo opäť prostredníctvom emailu. Vznikajú tým reťazové či lavínové správy. [7, 8]

Najčastejšie sa v prípade hoaxu teda jedná o správy typu:

- **Varovanie pred vírusmi v počítačmi**
    - Jedná sa o najčastejší druh hoaxu, ktorý sa môže v emailovej schránke objaviť. Odosielateľ dúfa v to, že príjemca tohto emailu sa takéhoto varovania zľakne a rozhodne sa stiahnuť si do počítača nejaký antivírusový program. Odkaz na takýto program, ktorý zistil, že práve v počítači užívateľa sa nejaký vírus nachádza je zväčša priložený taktiež. V niektorých prípadoch sa môže jednať o odkaz na skutočný antivírusový program, môže sa tiež ale stať, že užívateľ miesto toho, aby si do počítača nainštaloval antivírus, stiahne nejaký iný škodlivý kód, na ktorý bude práve antivírusový program potrebovať. [7]
- **Hrozba pred neexistujúcim nebezpečím**
    - Cieľ týchto správ, ktoré obsahujú vo väčšine prípadov lži, popr. vymyslené veci je vyvolať strach a paniku v neznalých užívateľoch. Jedná sa čisto o falošné správy určené práve na vyvolanie strachu v príjemcovi alebo v skupine príjemcov, popr. môže ísť o žart zo strany odosielateľa. [7]
- **Prosby o pomoc**
    - Môže sa jednať o skutočné prosby o pomoc, ktoré už nie sú aktuálne a môžu sa šíriť už len za účelom žartu, kedy sa odosielateľ snaží zaútočiť na ľudské city a vyvolať u príjemcu takéhoto emailu zlé pocity. Vo väčšine prípadov takéto správy už aktuálne nie sú, môže sa tiež ale stať, že je takáto prosba reálna a aktuálna. [7]
- **Petície, výzvy a zbieranie osobných údajov**
    - V emailovej schránke môže skončiť email, v ktorom odosielateľ žiada od príjemcu podpis na petíciu, ktorá sa napr. snaží proti niečomu bojovať. Takáto petícia môže byť čisto vymyslená a môže sa teda jednať o petíciu za vymyslenú vec, pričom bežný, neskúsený užívateľ si neoverí, či je petícia skutočná a osobe, ktorá túto petíciu poslala, pošle spätne svoje osobné údaje, v horšom prípade aj podpis. Tieto údaje môžu byť nasledovne preposlané niekam inam, kde môžu byť využité, ale tiež zneužité. Text petície totiž môže byť kedykoľvek zmenený aj bez vedomia užívateľa, ktorý tento podpis poskytol a môže sa tak stať, že podpis aj s osobnými údajmi môžu skončiť u petície či dokumentu, s ktorým vôbec nesúhlasí. [7]

- **Reťazové správy**
    - Do kategórie reťazových správ patria také správy, ktoré obsahujú určité múdrosti, porekadlá, popr. hromadne posielané žartovné emaily od rodinných známych či priateľov. Takýto druh správy často nabáda užívateľa k tomu, aby tento email rozposlal ďalej. [7]

V akomkoľvek z vyššie uvedených prípadov nie je vhodné a bezpečné akýkoľvek program na ochranu sťahovať, prispievať na organizácie alebo osobám, ktoré nie sú dôveryhodné, popr. dávať svoj podpis cudzím osobám a následne takúto správu šíriť ďalej.

1.4 Scam

Scam je nejaká podvodne navrhnutá schéma alebo taktika, vymyslená jednotlivcom alebo skupinou ľudí, ktorí sa nazývajú scameri. Snaha týchto útočníkov je získať určitý finančný obnos alebo čokoľvek, čo má nejakú hodnotu. Scameri sa snažia narušiť dôveru svojej obete, kde útočník sa vykresľuje ako niekto, kto má určité slovo alebo autoritu, teda vydáva sa napr. za investora, právnika, politika a pod. Scam je vlastne určitý druh podvodu, ktorý sa časom zdokonaľuje a útočníci vymýšľajú stále nové metódy, ktorými by mohli od svojich obetí dostať obnos peňazí. Typickým druhom scamu sú podvody s lotériami, falšovanie emailov, žiadosti o pomoc a pod. Najčastejším druhom scamu je pharming a phishing. [9]

1.4.1 Blackmailing

Jedná sa o vydieračské emaily, ktoré sa radia do kategórie scamu. Tieto emaily sú tiež nazývané webkamerové vydieranie alebo sextortion scam. Tieto druhy emailu obvykle končia automaticky v spamovom koši emailovej schránky, pričom takýchto emailov bolo za roky od ich vzniku poslaných niekoľko stoviek miliónov. Útočník pošle svojej obeti email, v ktorom obeť vydiera na poslanie určitej sumy peňazí na účet útočníka, najčastejšie v mene bitcoin, ktorá je popísaná v sekcii 1.8. V prípade, že by tak obeť neurobila, útočník rozpošle video a osobné údaje všetkým kontaktom, ktoré sú uložené na emailovej adrese obete. Len pár ľudí, ktorí obdržia takýto email platbu skutočne vykonajú. Rozposielanie takýchto emailov útočníkov nestojí žiadne finančné prostriedky, existuje však možný zisk pre útočníkov a preto sa tento druh scamu vyskytuje čoraz častejšie. [10]

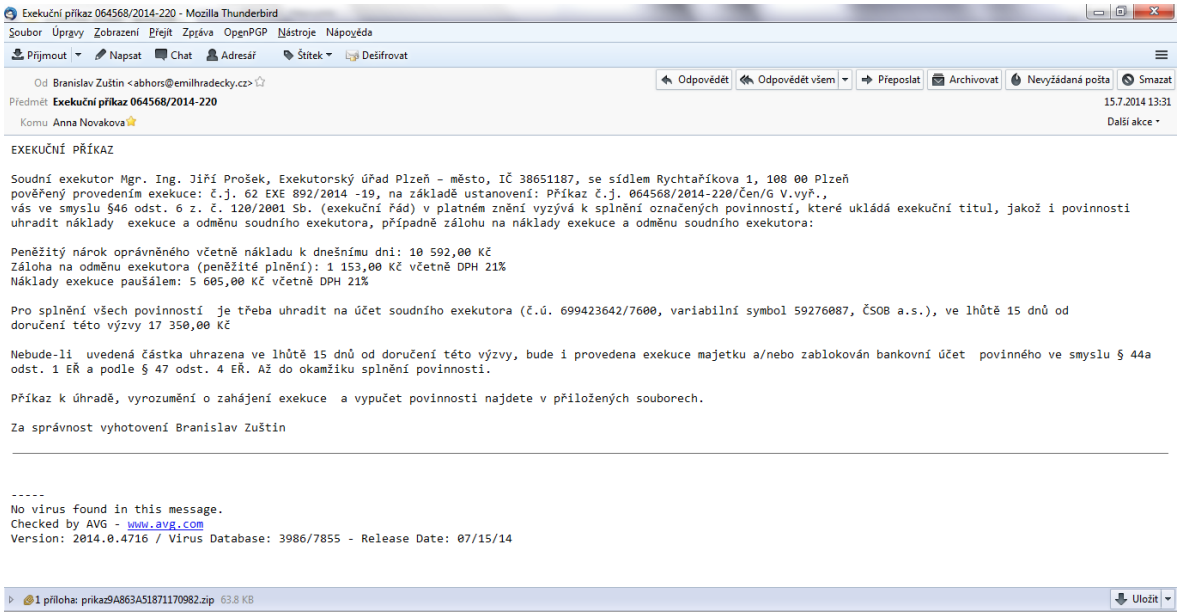
1.5 Phishing

Pod pojmom phishing sa rozumie činnosť odosielania veľkého množstva emailov užívateľom za účelom získania určitých informácii od príjemcov takýchto emailov. Tieto emaily zväčša pôsobia dôveryhodne a snažia sa užívateľa presvedčiť k odoslaniu osobných informácii, popr. k ovplyvneniu užívateľa. Definícia phishingu a rozdiel medzi obyčajným spamových emailom a phishingom je dostupná na blogu QuickHeal. Presná definícia podľa blogu znie: „*Ten najväčší rozdiel medzi spamom a phishingovým emailom je ten, že spamy nie sú vytvorené za účelom získania citlivých informácii o užívateľovi*“. [11]

Phishing je kombinácia sociálneho inžinierstva a technického podvodu. Phishingový email môže obsahovať súbor, ktorého cieľom je poškodiť užívateľa, teda po spustení takéhoto súboru by sa do počítača mohol vložiť malvér alebo iný škodlivý kód. Takýto email môže taktiež obsahovať odkaz na internetovú stránku. Tieto stránky sú zamerané na podvedenie užívateľa, ktorý tak bez svojho plného vedomia stiahne škodlivý softvér, popr. odovzdá útočníkovi svoje osobné informácie. Formou takéhoto útoku môže byť tiež spear phishing, v ktorom sa útočníci zameriavajú na jednotlivca, popr. malú skupinu ľudí. Útočníci si najskôr zistia dôležité informácie o svojej obeti a následne jej posielajú správy, ktoré môžu byť osobné alebo relevantné. Z tohto dôvodu je spear phishing zložitejší na rozpoznanie, naviac je ťažšie brániť sa mu. [11]

Každý užívateľ, ktorý aktívne využíva svojho emailového klienta, môže obdržať email od osoby, ktorú nepozná alebo o nej nepočul. Táto osoba sa od užívateľa môže snažiť získať osobné údaje tým, že sa vydáva za nejakú dôležitú inštitúciu, napr. banku. Ak užívateľ služby tejto banky využíva, môže byť emailom podvedený a v domnienke, že sa jedná o pravý email z jeho banky odošle spätne svoje citlivé osobné údaje, ako sú napr. meno, adresa, číslo karty, overovací kód karty, jej platnosť a pod., pričom môže dôjsť k strate peňažnej hotovosti alebo k ukradnutiu identity. [11]

Príkladom takéhoto emailu môže byť email od exekučnej spoločnosti. V obsahu tohto emailu môže byť napísaný text od dôveryhodnej osoby, ktorá sa reprezentuje ako exekútor, ktorý bol na užívateľa poslaný kvôli neplateniu úveru či hypotéky. Príklad takéhoto emailu je možné vidieť na obrázku 1:



Obrázok 1 – Príklad phishingového emailu, prevzatý zo stránky support.zcu.cz

Z emailu, ktorý je znázornený na obrázku 1, nemusí byť na prvý pohľad úplne jasné či sa jedná o phishing alebo nie. Samotný obsah emailu tak nepôsobí, keďže v texte sa nevyskytujú žiadne pravopisné chyby, adresa odosielateľa môže byť reálna a pod. Problém, ktorý sa v tejto správe vyskytuje môže byť príloha. Táto príloha je veľmi podozrivá, keďže sa v nej nachádza archív, v ktorom je uložený spustiteľný súbor s príponou .exe. Otvorenie takéhoto súboru by mohlo viesť k inštalácii škodlivého softvéru do počítača, čo by mohlo viesť k strate údajov alebo k znefunkčneniu počítača. Exekučná spoločnosť samotná by nikdy spustiteľný súbor neposlala. Takéto spoločnosti najčastejšie posielajú dokumenty a to vo formátoch .pdf alebo .doc. Útočník sa v takomto prípade spolieha na to, že neznalý alebo starší užívateľ, ktorý takýto email obdrží môže kvôli strachu tieto peniaze na účet odoslať, popr. otvorí priložený súbor zo strachu z exekúcie. V obidvoch prípadoch by tak vyhral útočník, ktorý by trebárs získal finančný obnos peňazí alebo by mohol prevziať kontrolu nad počítačom užívateľa. V skutočnosti sa jedná o typický, ale veľmi dobre premyslený phishingový útok, ktorý pracuje na princípe vyvolania strachu vo svojej obeti. [11]

1.5.1 Spear phishing

Spear phishing, rovnako ako obyčajný phishing, je emailová komunikácia s rovnakým cieľom, nie je však mierená na väčšie množstvá ľudí, ale len na jednotlivca či organizáciu. Aj keď cieľom útočníka je hlavne získanie finančného obnosu alebo citlivých osobných dát, útočníci môžu mať tiež v úmysle inštalovať škodlivý kód v počítači obete. Útočníci sa touto

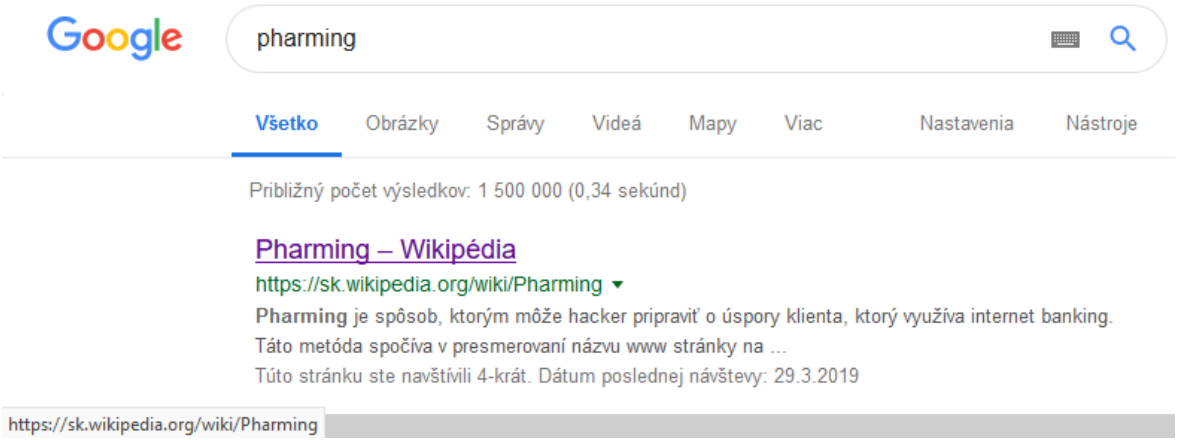
cestou taktiež snažia získať informácie o osobe, na ktorú útočia. K týmto informáciám môže patriť napr. adresa, meno zamestnávateľa, mená priateľov alebo lokácie miest, ktoré bežne navštevujú, no taktiež môže ísť o nejaký zoznam vecí, ktoré si obeť v poslednej dobe kúpila cez internet. Útočníci sa s takto získanými údajmi maskujú za priateľov alebo známych svojej obete, čím sa stávajú viac dôveryhodnými a snažia sa tak získať veľmi citlivé informácie, zväčša cez email. [12,13]

Spear phishing je často zameniteľný práve s phishingom kvôli tomu, že aj keď majú obidva tieto druhy útokov za cieľ získať informácie, ale u spear phishingu sa snaží útočník získať informácie od ľudí, u ktorých tuší, že to má cenu.

1.6 Pharming

Pharming, inak nazývaný aj pharmárčenie, je neologizmus založený na dvoch slovách, konkrétne na slovách farmárčenie a phishing, z ktorého vychádza. Pod týmto pojmom sa rozumie kybernetický útok, ktorého cieľom je vytvoriť stránku identickú k stránke reálnej, ktorá má rovnaký vzhľad a približne rovnaké funkcie, je v nej ale skrytý škodlivý kód, popr. nejaký vírus. Takýto malvér, ktorý sa môže na stránke nachádzať, môže byť použitý pre nainštalovanie počítačového vírusu, alebo tiež môže byť určený pre zachytenie každého stlačenia klávesu, ktoré užívateľ vykoná. Taktiež sa môže jednať o nainštalovanie nejakého softvéru, ktorý môže útočník použiť k tomu, aby diaľkovo prevzal kontrolu nad počítačom po dobu našej neprítomnosti a pod. Tieto útoky sa v minulosti zvykli vyskytovať hlavne na stránkach s nevhodným obsahom, popr. na pochybných stránkach. Takýto malvér sa môže často vyskytovať na stránkach s obsahom pre dospelých, na stránkach s hazardom, teda internetových kasínach a pod. [14,15]

V súčasnosti sa tento typ útokov rozširuje aj na iné stránky, ktoré majú dôležitý obsah a nijak sa neradia do zoznamu pochybných stránok. Jedná sa napr. o stránky banky, úradov a pod. Veľké množstvo ľudí má problém rozoznať, či sa jedná práve o stránku skutočnú alebo jej napodobeninu. Problém je práve v tom, že pred otvorením takéhoto odkazu si užívateľ nezvykne overiť či odkaz, ktorý práve otvoril vedie na stránku skutočnú. Jedným z riešení ako overiť, či je stránka skutočná je označiť kurzorom myši túto stránku v akomkoľvek vyhľadávacom mechanizme (napr. Google) a v ľavom dolnom rohu si overiť, či sa odkaz pre presmerovanie zhoduje s odkazom uvedeným pod stránkou. Príklad takéhoto overenia je možné vidieť na obrázku 2:



Obrázok 2 – Overenie odkazu pre kontrolu pharmingu

V prípade, ktorý je znázornený na obrázku 2 sa odkaz zhoduje so stránkou, ktorú chceme prehľadávať. Môže sa však stať, že odkaz by viedol na nejakú inú stránku, čo je príznak pharmingu a v takomto prípade by sa užívateľ mal vyhnúť návšteve tohto odkazu. [14,15]

Pharming samotný sa v posledných rokoch stáva veľkým problém práve e-komercii a internet bankingu. Užívatelia týchto služieb na týchto stránkach zdieľajú svoje dôležité osobné informácie, napr. čísla kreditných kariet, adresy a pod. Z tohto dôvodu bol navrhnutý systém antipharming, čo je sofistikovaný spôsob ochrany týchto stránok pred vážnou hrozbou pharmingu. Samotný antivírusový program ani odstraňovač spyware softwaru v počítači nedokáže užívateľa ochrániť pred pharmingom. [14]

1.7 Nigerian 419

Tento typ spamových emailov je veľmi častý, veľakrát sa rovnaké správy aj opakujú, pričom niektoré z nich sú dostatočne dôveryhodné na to, aby osoba, ktorá takýto email dostala, obsahu uverila a splnila všetko to, čo odosielateľ žiada. V prípade takéhoto typu spamového emailu sa jedná o to, že odosielateľ sa prezentuje ako osoba zo zámoria alebo z nejakej veľmi ďalekej krajiny a ponúka príjemcovi správy obrovské množstvo peňazí, častokrát aj nejaké dedičstvo. Výmenou za to žiada o pomoc s presunom peňazí mimo krajiny odkiaľ pochádza. Tento druh prišiel pôvodne z Nigérie, podľa čoho aj nesie názov. V dnešnej dobe je možné takýto email dostať z akéhokoľvek miesta na svete. [16]

Tento typ útoku môže prísť listovou zásielkou, SMS správou, správou na sociálnych sieťach, najčastejšie sa však vyskytuje práve cez email. Scamer, teda osoba, ktorá sa takto snaží napáliť čitateľa, sa snaží rozrozprávať nejaký príbeh o tom, že v banke uviazli peniaze následkom vojny alebo iných okolností. Tvrdí, že patrí k našej dlho stratenej rodine a chce

nám ako svojmu blížnemu pomôcť s financiami. V obidvoch spomenutých prípadoch to vedie k tomu, že odosielateľ tohto emailu žiada od čitateľa určité množstvo peňazí, aby sa mohol k uzamknutým peniazom v banke dostať, kvôli daniam a pod. Žiadajú takto o pomoc dostať tieto peniaze z krajiny, v ktorej momentálne sú a sľubujú za to veľkú finančnú odmenu. Tieto emaily však v ani jednom zo spomenutých prípadov nie sú reálne a ich cieľom je nalákať príjemcu na víziu rýchleho bohatstva. Útočník sa spolieha na to, že práve tejto vízii určité množstvo ľudí podľahne a peniaze na účet pošle. Práve druhý typ tejto správy, v ktorej sa útočník prezentuje ako stratený rodinný príbuzný, ktorý je v núdzi a potrebuje financie, je zameraný na útok na ľudské city a na ľútosť, popr. na strach o svojho blížneho. V takýchto situáciách väčšina ľudí nepremýšľa nad tým, či takýto príbuzný skutočne existuje a v dobrej viere žiadanú sumu skutočne pošlú. Pravdou však je to, že takýto stratený príbuzný nikdy neexistoval a jedná sa len o obohatenie na úkor obete útoku. [16]

1.7.1 Varovné signály, že sa môže jednať o scam

Môže byť niekoľko varovných signálov toho, že scam, ktorý skončil v emailovej schránke patrí práve do kategórie Nigerian 419. Najčastejšie sa môže jednať o tieto varovné signály:

- Užívateľ je kontaktovaný osobou, ktorá pochádza z krajiny ako je napr. Irak, Irán, Nigéria a pod. s tým, že táto osoba žiada previesť peniaze z tuzemska do krajiny príjemcu takéhoto emailu. [17]
- Zväčša býva priložený dlhý a tiež smutný príbeh o tom, prečo a konkrétne z akého dôvodu nemôžu byť tieto peniaze prevedené ich skutočným majiteľom. Zvykne sa jednať o problémy s dedičstvom, popr. iný konflikt, a preto chce odosielateľ poslať peniaze priamo na bankový účet príjemcu. [17]
- Útočník následne navrhne finančnú odmenu za pomoc s prevedením takto uväznenej finančnej hotovosti. Odmenou býva najčastejšie podiel z tejto čiastky, pričom jej hodnota môže byť obrovská, konkrétne milióny eur či dolárov. [17]
- Pre získanie tohto finančného obnosu útočník žiada o poslanie nejakej sumy na uvedený bankový účet. Dôvodom zväčša býva to, že je potrebné zaplatiť banke za tento prevod, právnikovi za právne kroky alebo zaplatenie vládnej agentúre. Scamer touto cestou žiada o zaplatenie uvedenej sumy cez bankový prevod, čo vedie k strate tejto sumy zo strany obete. [17]

1.8 BITCOIN

„*Bitcoin je kolekcia konceptov a technológií, ktoré formujú základňu digitálneho peňažného ekosystému. Jednotky tejto meny, nazývané bitcoin, sa používajú k ukladaniu a prenášaniu hodnoty medzi účastníkmi bitcoinovej siete*.“ [18]

Pod pojmom bitcoin si bežný užívateľ môže predstaviť dve veci:

1. Virtuálnu menu
2. Systém platieb používaný pre prijímanie a posielanie peňazí cez internet.

Samotná mena je dôležitá, no rovnako dôležitý je aj systém jej platieb. Bez tohto premysleného systému by mena samotná fungovať nemohla. [18, 19]

1.8.1 Bitcoin ako mena

Bitcoin je digitálna, pseudoanonymná, Peer-to-Peer a decentralizovaná mena. Digitálna je kvôli tomu, že samotný bitcoin existuje vo svete len ako kód, nepatrí teda medzi zoznam mien, ktoré je možné pri sebe fyzicky držať. V minulosti sa objavili určité pokusy o prevod tejto meny na menu fyzickú, tieto pokusy však dopadli neúspešne. [17]

To, že je mena pseudoanonymná znamená, že aj keď je možné vidieť všetky bitcoinové transakcie v tzv. Blockchaine, samotný odosielateľ a prijímateľ sú známi len ako určité reťazce náhodných znakov a čísiel. Používanie bitcoinu môže byť plne anonymné v prípade, že užívateľ presne vie, ako sa táto mena používa. Práve toto je jeden z dôvodov, prečo je bitcoin používaný najčastejšie práve hackermi a útočníkmi, ktorí žiadajú finančné obnosy práve v tejto mene. Spoliehajú sa na to, že nie je jednoduché, popr. možné ich vypátrať. [17, 18]

Pod pojmom decentralizovaná mena sa myslí to, že pre túto menu nie je vytvorená žiadna banka ani inštitúcia, ktorá by túto menu ponúkala či riadila. Za menu je zodpovedná skupina jedincov, ktorí program a virtuálne-peňažný systém udržiavajú v prevádzke. Slovné spojenie Peer-to-Peer značí to, že každý jednotlivec, ktorý bitcoin má ho aj skutočne vlastní. Nikto iný k tomuto konkrétnemu bitcoinu prístup nemá a nikto si ho nemôže nijak privlastniť. V prípade, že sa vlastník tohto bitcoinu rozhodne, že ho odošle niekomu inému, je tento bitcoin poslaný priamo inej osobe. Keďže bitcoin ako menu nespravuje žiadna banka či organizácia alebo inštitúcia, posielanie ide priamo z jedného vlastníka na druhého, čím sa zabráni napr. tomu, aby si banka privlastnila nejakú jeho časť za prevod. [17]

Bitcoin je prvá digitálna mena spĺňajúca tieto charakteristiky. Keďže je táto mena založená na kryptografii, jej sila spočíva hlavne v kóde, ktorý používa extrémne silnú kryptografiu k zaisteniu toho, aby sa k bitcoinom nedostal nikto bez vedomia vlastníka, popr. jeho povolenia. Keďže bol bitcoin vyvinutý ako prvá skutočne fungujúca virtuálna kryptomena, viedlo to k tomu, že práve on zaznamenal najväčší úspech. Jeho hodnota nebola v začiatkoch veľká, postupom času sa však zdokonaľoval a v časoch najväčšej slávy mal hodnotu takmer 20 tisíc dolárov. [17, 18]

1.8.2 História bitcoinu

Aj keď bol bitcoin prvá stabilná a hodnotná virtuálna kryptomena, ktorá mala skutočný úspech, mal aj svojich predchodcov. Pokusy o vytvorenie online meny, ktorá bude šifrovaná, boli už predtým, príkladmi môžu byť B-Money a BitGold. Tieto meny boli sformulované, ale nikdy neboli dotiahnuté do konca. Vývojár pod prezývkou Satoshi Nakamoto sa z tých chýb poučil a roku 2008 bol na fórum o kryptografii pridaný príspevok „Bitcoin – Elektronický peňažný Peer-To-Peer systém“. Tento príspevok bol práve od Satoshiho, nikdy sa ale nezistilo, či toto meno patrilo skutočnej osobe, či sa jednalo o prezývku alebo či išlo o skupinu vývojárov. [18, 19]

Aj keď Bitcoin ako software bol uvedený na verejnosť prvýkrát až v roku 2009 a jeho prvé ťaženie, teda spôsob, akým sa bitcoin získava, bolo zahájené tiež tohto roku, prvú hodnotu mala táto mena až o rok pozdejšie. Spôsobené to bolo tým, že táto mena nebola nikdy používaná a neprebehla s ňou žiadna platba, bol totiž len ťažený, ale nevyužívaný. Kým ním neprebehla žiadna platba, nebolo možné mu priradiť akúkoľvek trhovú hodnotu. Práve v roku 2010 sa niekto rozhodol, že bitcoin využije ako platidlo a zaplatil 10000 jednotiek tejto meny výmenou za 2 pizze. Ak by sa majiteľ týchto bitcoinov v minulosti nevzdal, mohol mať pri sebe hotovosť 200 miliónov dolárov v čase, keď bitcoin zaznamenal svoje maximum. [19]

O rok pozdejšie, roku 2011, popularita bitcoinu silne rástla a nápad decentralizovanej a silne zabezpečenej kryptomeny sa niesol aj ďalej, kde sa konkurenti rozhodli vytvoriť ďalšie kryptomeny. Všetky sa snažili vylepšiť dizajn bitcoinu a zlepšiť tým kľúčové aspekty ako zabezpečenie, anonymitu či rýchlosť. V súčasnosti je používaných viac ako 1000 kryptomien, z čoho väčšina vznikla práve ako reakcia na najznámejší bitcoin. [19]

Hodnota bitcoinu sa s rastúcim záujmom zvyšovala, až do roku 2013, v ktorom bitcoin dosiahol hodnoty 1000 dolárov po prvýkrát. Onedlho na to jeho hodnota však začala opäť klesať, konkrétne o niekoľko stoviek dolárov, až kým sa toto klesanie nezastavilo na hodnote 300 dolárov. Tento pokles, ale celkovo aj anonymitu tejto meny považovali hackeri a spameri za svoju výhodu a preto sa rozhodli, že finančné obnosy budú od svojich obetí žiadať práve v tejto mene. S vedomím, že sú reprezentovaní ako reťazec znakov a čísiel a teda nemôžu byť vystopovaní, podnikli hackeri útok na Mt.Gox, najväčšiu bitcoinovú zmenáreň, odkiaľ ukradli 850 tisíc bitcoinov, ktoré už nikto nevidel. Ich hodnota by v čase najvyššej hodnoty bitcoinu bola takmer 17 miliárd dolárov. [19]

Od útoku na túto spoločnosť cena bitcoinu kolísala len mierne, no útočníci, ktorí v tejto mene stále videli potenciál, či už kvôli nestabilnej hodnote alebo kvôli anonymite, ju používali aj naďalej. V roku 2017 dosiahol bitcoin svoje maximum, pričom práve začiatkom tohto roka cena jedného bitcoinu stúpla nad tisíc dolárov. Ceny sa stále menili, takmer vôbec však neklesali, až do decembra roku 2017, kedy bitcoin dosiahol svoje úplné maximum a jeho hodnota sa pohybovala okolo 20 tisíc dolárov za jednu jednotku tejto meny. Dosiahnuté to bolo hlavne tým, že o túto menu začali mať záujem banky a inštitúcie, ktoré hľadali cestu k tomu, ako by bolo možné túto menu implementovať do svojho platobného systému. Technológia Blockchain, ktorá stála za bitcoinom, medzitým zaznamenala mimoriadny úspech, kde sa dalo hovoriť až o revolúcii v oblasti finančných technológií. Od decembra roku 2017 však cena bitcoinu len klesala, pričom v čase, keď dosiahol minimálnu hodnotu mal cenu len niečo málo cez 3 tisíc dolárov. [19]

1.8.3 Bitcoinové peňaženky

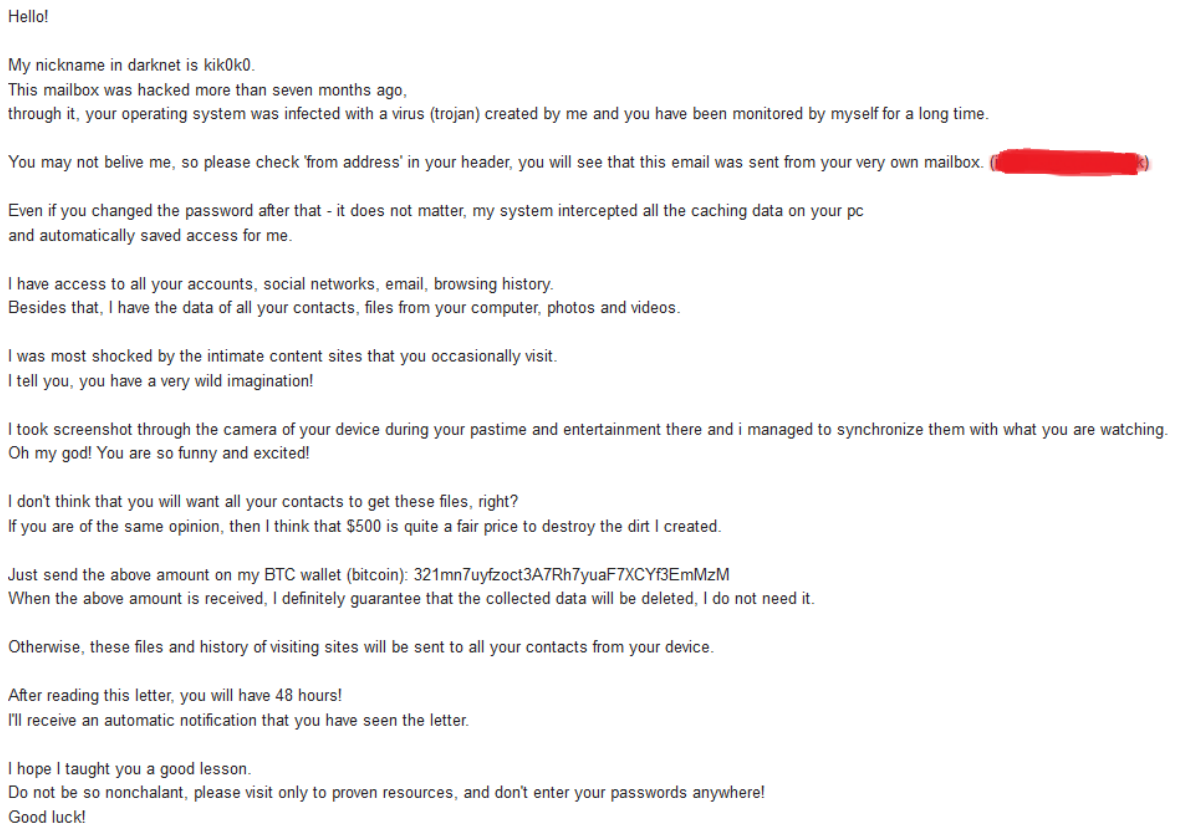
Bitcoiny je možné po vyťažení držať na počítači, SIM karte, v telefóne, tablete alebo na prenosnom disku. Existuje ale istá šanca, že takéto zariadenie sa môže pokaziť alebo stratiť, čím by vlastník prišiel o všetky nadobudnuté bitcoiny. Tento problém sa vývojári snažili vyriešiť, pričom prišli s nápadom vytvorenia peňaženky pre túto menu. Od implementácie tohto návrhu je možné si uložiť svoje vyťažené bitcoiny na bitcoinovú peňaženku, ktorá je umiestnená v internetovom cloude. Informácie z nej je možné si zálohovať na prenosné zariadenie, napr. na telefón, USB alebo na prenosný počítač, kde pri zálohovaní budú tieto informácie správne zašifrované, čím sa predíde k zneužitiu alebo krádeži uloženej sumy. Kľúč samotný drží len vlastník peňaženky, môže ho však zdieľať s inou osobou, ktorej verí. Táto osoba následne môže odkryť informácie o tejto peňaženke. [20]

Každá bitcoinová peňaženka má svoju vlastnú bitcoinovú adresu. Akonáhle užívateľ nejaké bitcoiny vyťaží, alebo sa rozhodne ich kúpiť, či naopak predať, použije práve túto adresu. Typickým vzorom tejto adresy môže byť 321mn7uyfzoct3A7Rh7yuaF7XCYf3EmMzM. Adresu a peňaženku je možné si zriadiť na viacerých stránkach, teda u viacerých poskytovateľov. V jednom čase je možné vlastniť viac peňaženiek, pričom sa odporúča mať jednu peňaženku pre kupovanie bitcoinov a druhú pre ich následný predaj. [20]

1.8.4 Používanie bitcoinu u útočníkov

Práve v anonymite bitcoinu vidia potenciál mnohí útočníci. Tým, že je takmer nemožné vypátrať, komu adresa patrí a taktiež vďaka tomu, že je služba Peer-to-Peer, teda do toho nezasahuje žiadna banka ani iná inštitúcia stojaca uprostred, je táto mena príliš obľúbená práve útočníkmi. Útočníci takto mesačne získavajú desiatky tisíc dolárov, pričom väčšinou dochádza k phishingu a scamu, teda k žiadaniu financií od bežného užívateľa práve cez poslané emaily. Odhaduje sa, že až 30% z týchto financií pochádzajú zo scamu cez email. [21]

Takýto vydieračský email je možné obdržať aj vtedy, ak vlastník emailovej schránky nenavštevuje žiadne pochybné alebo nevhodné stránky. Zapríčinené to môže byť tým, že napr. diskusné fórum, na ktoré sa užívateľ registroval, bolo podrobené útoku hackerov, ktorí ukradli osobné údaje veľkého množstva registrovaných užívateľov, teda napr. údaje ako meno, priezvisko, email, ktorý bol pri registrácii použitý, občas taktiež aj heslo použité pri registrácii. Email získaný z databázy útočníci následne využijú k tomu, aby naň poslali výhražný mail, ktorý môže byť napísaný v rôznych jazykov, najčastejšie však v jazyku anglickom. Príklad takéhoto emailu je možné vidieť na obrázku 3:



Hello!

My nickname in darknet is kik0k0.
This mailbox was hacked more than seven months ago,
through it, your operating system was infected with a virus (trojan) created by me and you have been monitored by myself for a long time.

You may not belive me, so please check 'from address' in your header, you will see that this email was sent from your very own mailbox. ([redacted])

Even if you changed the password after that - it does not matter, my system intercepted all the caching data on your pc
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Besides that, I have the data of all your contacts, files from your computer, photos and videos.

I was most shocked by the intimate content sites that you occasionally visit.
I tell you, you have a very wild imagination!

I took screenshot through the camera of your device during your pastime and entertainment there and i managed to synchronize them with what you are watching.
Oh my god! You are so funny and excited!

I don't think that you will want all your contacts to get these files, right?
If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created.

Just send the above amount on my BTC wallet (bitcoin): 321mn7uyfzoct3A7Rh7yuaF7XCYf3EmMzM
When the above amount is received, I definitely guarantee that the collected data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will be sent to all your contacts from your device.

After reading this letter, you will have 48 hours!
I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Obrázok 3 – Príklad vydieračského emailu poslaného na adresu autora práce

Z obrázku 3, kde je takýto vydieračský email zobrazený v anglickom jazyku. Jedná sa o typický vydieračský email, v ktorom sa útočník užívateľovi predstaví a oznámi mu, že jeho systém bol infikovaný škodlivým vírusom, ktorý vytvoril. Útočník následne vyzýva užívateľa k tomu, aby si skontroloval adresu, z ktorej tento email prichádza. Práve tento druh vydieračských emailov zvyšuje strach v užívateľovi tým, že email odosielateľa prišiel z emailovej schránky, v ktorej aj skončil. Útočník následne varuje užívateľa o tom, že získal prístup ku všetkým osobným údajom zo všetkých účtov, ktoré obeť vlastní. Tieto údaje zo svojho počítača zmaže len v prípade, že mu jeho obeť pošle určitý obnos peňazí, zväčša uvedený v dolároch, na jeho bitcoinovú peňaženku v bitcoinoch. V prípade, ak by tak obeť nespravila sa útočník vyhráža zverejnením týchto osobných údajov, teda napr. intímnych fotiek, ktoré spravil kým bola obeť nepozorná, zverejnenie konverzácii, ktoré ukradol zo sociálnych sietí a pod. Následne útočník poskytne svoju bitcoinovú peňaženku, na ktorú má obeť predom stanovené peniaze poslať. Útočník dostane upozornenie na to, že tento vydieračský email užívateľ otvoril a na to nadväzuje varovanie pre obeť, ktorá ak peniaze neodošle do 48 hodín od otvorenia na peňaženku útočníka, príde o svoje citlivé údaje. [21]

Útočníci sa v prípade takýchto vydieračských emailov spoliehajú na svoju najväčšiu výhodu, ktorou je vyvolanie strachu vo svojej obeti, ktorá môže tieto peniaze na účet poslať. V skutočnosti sa jedná o druh scamu, kde sa útočník priam spolieha na nevedomosť a strach obetí, pričom žiadne upozornenie o otvorení emailu nedostane a taktiež žiadne osobné údaje nevlastní. V prípade, že by obeť žiadanú finančnú sumu odoslala, by umožnila ďalším útočníkom ďalšie vyhrážanie, pretože by v nej útočníci videli potenciál.

2 NÁVRH RIEŠENIA KATEGORIZÁCIE

Pri riešení návrhu kategorizácie spamových emailov sa vychádzalo z teórie, ktorá bola popísaná v prvej kapitole práce. Pred začatím samotného návrhu bolo potrebné si objasniť metódy, akými fungujú pharming, phishing a hlavne to, ako fungujú bitcoinové peňaženky a ako vypadajú vydieračské emaily. Keďže práve tieto vydieračské emaily, kde útočníci žiadajú sumu peňazí v bitcoinoch sú veľkou hrozbou, je dôležité tomu prispôsobiť aj návrh a následnú realizáciu tohto návrhu. Celkový počet emailov, ktoré boli pre túto bakalársku prácu poskytnuté je 41072, čomu bude potrebné prispôsobiť aj celú etapu realizácie. Cieľom celého procesu je dosiahnuť to, aby boli vytvorené skripty čo najuniverzálnejšie, pričom budú ignorovať chyby v emailoch, čím sa predíde nesprávnej kategorizácii a ukončeniu celého skriptu.

Program na kategorizáciu bude rozdelený do viacerých častí, kde sa budú postupne získavať všetky dôležité alebo vyhovujúce údaje, ktoré by bolo možné následne použiť pre čo najlepšiu štatistiku z týchto emailov. Hlavným cieľom bude zistiť IP adresu z obsahu emailu, pomocou ktorej bude následne možné zistiť miesto, odkiaľ email približne pochádza, teda krajinu pôvodu. Následne bude vykonané overenie, či poslaný email obsahoval aj nejaký súbor ako prílohu, pričom bude použitých viacero možných koncoviek. Ďalej sa v emailovom súbore vyhľadajú kľúčové slová, aby sa zistilo, či má email vydieračský charakter, popr. či obsahuje odkaz na nejakú stránku. Priame zistenie, či sa jedná o phishing alebo pharming je príliš zložité a náročné na realizáciu, preto bude zistený počet odkazov, čím sa môže utvoriť aspoň približný pohľad na to, koľko emailov môže byť phishing alebo pharming potenciálne a koľko emailov môže približne viesť na podvodnú stránku.

2.1 Zistenie IP adresy

Prvým krokom pre kategorizáciu emailov bude zistenie IP adresy, keďže z tejto unikátnej adresy je ďalej možné zistiť množstvo informácii ako napr. krajinu, z ktorej email pochádza, alebo či sa takáto adresa neobjavuje na čiernom zozname, tzv. blackliste. Zistiť adresu priamo zo súboru je možné viacerými spôsobmi, predpokladá sa však, že v súbore sa bude IP adries vyskytovať väčšie množstvo. Pre vyhľadávanie adresy v súbore by bolo najvhodnejšie použiť regulárne výrazy, taktiež nazývané regex-y. Takéto výrazy predstavujú účinný spôsob vyhľadávania rôznych textových reťazcov v súboroch.

Po bližšom skúmaní emailových súborov, ktoré boli poskytnuté, je zrejmé, že v súbore sa nachádza viac takýchto adries, pričom vždy sa nachádzajú aspoň 3 adresy, vo väčšine prípadov 4 adresy, niekedy aj viac, pričom prvé adresy sú vždy adresy príjemcu, popr. adresa emailu, odkiaľ sa email preposlal a posledná adresa je vo všetkých prípadoch adresa odosielateľa. Pred adresami je podľa formátu .emlx súboru vždy kľúčové slovo **Received:**, malo by teda byť možné IP adresu nájsť tak, že za posledným výskytom tohto kľúčového slova sa bude v hranatých zátvorkách nachádzať práve IP adresa odosielateľa. Príklad takéhoto .emlx súboru je možné vidieť na obrázku 4:

```
      FROM_LOCAL_NOVOWEL,HTML_IMAGE_ONLY_
12,HTML_MESSAGE,HTML_SHORT_LINK_IMG_2,
      MIME_HTML_ONLY,RDNS_NONE,SPF_SOFTFAIL,URIBL_BLACK,URIBL_J
P_SURBL
      autolearn=spam version=3.2.3
X-Spam-Report:
 *  0.5 FROM_LOCAL_NOVOWEL From: localpart has series of non-
vowel letters
      *  0.6 SPF_SOFTFAIL SPF: sender does not match SPF record
(softfail)
      *  2.5 HTML_IMAGE_ONLY_12 BODY: HTML: images with
800-1200 bytes of words
      *  0.0 HTML_MESSAGE BODY: HTML included in message
      *  1.5 MIME_HTML_ONLY BODY: Message only has text/html
MIME parts
      *  1.5 URIBL_JP_SURBL Contains an URL listed in the JP
SURBL blocklist
      *      [URIs: xpozify.com]
      *  2.0 URIBL_BLACK Contains an URL listed in the URIBL
blacklist
      *      [URIs: xpozify.com]
      *  0.7 DNS_FROM_AHBL_RHSBL RBL: Envelope sender listed in
dnsbl.ahbl.org
      *  0.0 HTML_SHORT_LINK_IMG_2 HTML is very short with a
linked image
      *  0.1 RDNS_NONE Delivered to trusted network by a host
with no rDNS
      * -0.2 AWL AWL: From: address is in the auto white-list
Received: from mailbox.utb.cz (unknown [192.168.1.12])
      by sun.utb.cz (Postfix) with ESMTP id 4FEEB340129A1
      for <zacek@fai.utb.cz>; Fri, 31 Aug 2018 17:10:42 +0200
(CEST)
Received: by mailbox.utb.cz (Postfix, from userid 3000)
      id 420C47827EC1; Fri, 31 Aug 2018 17:10:42 +0200 (CEST)
Delivered-To: utb_ekonference@mailbox.utb.cz
Received: from sun.utb.cz (unknown [192.168.1.13])
      by mailbox.utb.cz (Postfix) with ESMTP id 0F99D7827EBE
      for <utb_ekonference@mailbox.utb.cz>; Fri, 31 Aug 2018
17:10:42 +0200 (CEST)
Received: by sun.utb.cz (Postfix, from userid 1000)
      id 0E4B4340D4FE3; Fri, 31 Aug 2018 17:10:42 +0200 (CEST)
Received: from elate.xpozify.com (elate.kevinjmccarthy.com
[185.125.231.54])
      by sun.utb.cz (Postfix) with ESMTP id CC905340129A5
      for <ekonference@utb.cz>; Fri, 31 Aug 2018 17:10:30 +0200
(CEST)
```

Obrázok 4 – Hľadanie IP adresy z obsahu emailového súboru

Takto nájdenú adresu by malo byť možné práve cez regex nájsť, vytiahnuť a uložiť do pamäte a súboru, aby s ňou bolo možné aj ďalej pracovať a aby z nej bolo možné zistiť

krajinu a jej kód. Keďže súborov je veľké množstvo, niektoré adresy by sa mohli opakovať, čomu bude potrebné prispôsobiť aj kód, ktorý overí, či už sa rovnaká adresa v zozname adries nenachádza. V prípade, že by adresa už v zozname existovala, k počtu výskytov tejto adresy by sa pripočítalo číslo 1.

2.1.1 Vyhľadanie krajiny

Pre vyhľadanie krajiny by bolo pravdepodobne najlepšie riešenie použitie nejakého API, najlepšie takého, ktoré je zdarma. Toto API bude slúžiť na vyhľadávanie krajiny, odkiaľ tento email bude pochádzať. K tomu bude použitý JSON, pomocou ktorého bude potrebné otvoriť nejakú webovú stránku, práve takú, ktorá obsahuje spomenuté API, ktoré adresu následne skontroluje a zistí z nej všetky potrebné informácie. Takéto služby, ktorých používanie nie je spoplatnené, však majú väčšinou nejaké obmedzenia, popr. nie sú najpresnejšie, na zistenie krajiny budú však postačujúce. Výsledkom kontroly budú JSON dáta, z ktorých bude potrebné zistiť údaj country, teda krajinu a údaj countryCode, čo značí kód krajiny. Pri použití adresy, ktorá je zobrazená na obrázku 4, je možné zistiť, že táto adresa pochádza z Ruska a má kód RU. Taktiež by bolo možné zistiť región a mesto, tieto údaje však nie sú až tak presné a použité nebudú. Výstup z JSON je možné vidieť na obrázku 5:

```
{
    "query": "185.125.231.54",
    "status": "success",
    "country": "Russia",
    "countryCode": "RU",
    "region": "MOW",
    "regionName": "Moscow",
    "city": "Moscow",
    "district": "",
    "zip": "",
    "lat": 55.8134,
    "lon": 37.5314,
    "timezone": "Europe/Moscow",
    "isp": "MAROSNET Telecommunication Company Network",
    "org": "",
    "as": "AS48666 MAROSNET Telecommunication Company LLC",
    "mobile": false,
    "proxy": false
}
```


Obrázok 5 – Dáta z JSON

Po zistení krajiny a kódu tejto krajiny bude možné pokračovať v kontrole ďalších údajov, ktoré budú potrebné pri kategorizácii, keďže všetky dôležité informácie z IP adresy už zistené sú. Problém pri vyhľadávaní krajín však môže byť to, že takmer všetky API, ktoré sú zdarma, majú svoje využitie limitované a obmedzené, či už sa to týka celkového počtu overení na deň alebo limit overení na minútu. Kvôli takémuto obmedzeniu bude potrebné nastaviť limit vyhľadávania IP adries na určitý počet tak, aby limit maximálnych vyhľadávaní nebol presiahnutý a následne vyvolať čakanie určitú dobu, ktorá bude stanovená podmienkami tohto API, čím sa predíde odstrihnutiu využívania takejto služby zdarma.

2.2 Zistenie súboru

Niektoré spamové emaily môžu pri príchode do emailovej schránky obsahovať aj dodatočný súbor ako prílohu, či už sa jedná o obrázky, dokumenty, archívy alebo spustiteľné súbory. Bude preto potrebné zistiť, či sa takéto súbory nachádzajú v prílohách a ak áno, aký je ich

počet. Takéto súbory v prílohách môžu obsahovať rôzne koncovky, napríklad .exe práve pre spustiteľné súbory, .doc, .docx alebo .pdf pre dokumenty, .png alebo jpg. pre obrázky, no taktiež sa tu môžu nachádzať aj .zip archívy. Práve v .zip archívoch sa môže vírus vyskytovať najčastejšie. Taktiež sa môžu vyskytovať aj súbory s inými koncovkami, zahrnuté však budú len koncovky najbežnejšie.

Hľadanie samotné bude pozostávať z toho, že sa bude hľadať meno súboru, teda reťazec **name = “ “** pomocou regex. Samotná podoba obsahu emailu, kde sú zobrazené prílohy je zobrazená na obrázku 6:

```
Received: from mailbox.utb.cz (unknown [192.168.1.12])
     by sun.utb.cz (Postfix) with ESMTP id 6AB3434094194
     for <zacek@fai.utb.cz>; Tue, 23 May 2017 19:56:12 +0200
(CEST)
Received: by mailbox.utb.cz (Postfix, from userid 3000)
     id 5EB7F78348EC; Tue, 23 May 2017 19:56:12 +0200 (CEST)
Delivered-To: utb_ekonference@mailbox.utb.cz
Received: from sun.utb.cz (unknown [192.168.1.13])
     by mailbox.utb.cz (Postfix) with ESMTP id DAB3278348EC
     for <utb_ekonference@mailbox.utb.cz>; Tue, 23 May 2017
19:56:11 +0200 (CEST)
Received: by sun.utb.cz (Postfix, from userid 1000)
     id D87A434094192; Tue, 23 May 2017 19:56:11 +0200 (CEST)
Received: from [45.124.4.159] (unknown [45.124.4.159])
     by sun.utb.cz (Postfix) with ESMTP id 2B6703409418A
     for <e-konference@utb.cz>; Tue, 23 May 2017 19:56:03 +0200
(CEST)
From: CARLA ERRAT <CARLA.ERRAT@RYANSTEELE.COM>
To: <e-konference@utb.cz>
Subject: [SPAM] Invoice(02-6709)
Date: Tue, 23 May 2017 23:26:01 +0530
Message-ID: <ejebomm$a5f3f7f0$qarjrgehj$@ryansteele.com>
Content-Type: multipart/mixed;
     boundary="----=_NextPart_000_001B_01CF346E.A5F3F7F0"
X-Mailer: Microsoft Outlook 14.0
X-Spam-Prev-Subject: Invoice(02-6709)
X-Spam-Prev-Subject: [SPAM] Invoice(02-6709)
MIME-Version: 1.0

------=_NextPart_000_001B_01CF346E.A5F3F7F0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

Thank you for your order.  Your Invoice - 02-6709 is attached.


------=_NextPart_000_001B_01CF346E.A5F3F7F0
Content-Type: application/pdf; name="02-6709.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="02-6709.pdf"
```

Obrázok 6 – Emailový súbor s prílohou

Z celého obsahu emailového súboru sa vyberie časť **name = “ “**, z ktorej sa následne zistí, o akú príponu súboru išlo. Vezme sa teda údaj, ktorý sa nachádza za bodkou, v prípade, ktorý je znázornený na obrázku 6 sa jedná o súbor s koncovkou .pdf. Taktiež by mohol byť použitý reťazec filename, ten sa ale nevyskytuje u všetkých takýchto súborov s prílohami.

2.3 Zistenie odkazov na iné stránky

Keďže pharming, popr. phishing je možné rozpoznať tak, že súčasťou emailu môže byť hypertextový odkaz, ktorého úlohou je po kliknutí nasmerovať užívateľa na nejakú stránku, kde by od neho mohlo byť vyžadované, aby vyplnil svoje osobné údaje, popr. by mu bola zobrazená nejaká reklama, no taktiež by bolo možné sa takto dostať na stránku obsahujúcu nebezpečný kód alebo súbor, ktorý by sa mohol automaticky začať sťahovať. Cieľom bude zistiť, či sa v súbore nejaké hypertextové odkazy nachádzajú. Predpokladá sa, že väčšina emailových súborov práve takéto odkazy obsahovať bude, či už budú viesť na stránku, ktorej platnosť skončila, alebo na stránku, kde sa vyskytuje reklama, popr. o podvodnú stránku.

Samotné vyhľadávanie hypertextových odkazov bude prebiehať pomocou regex, kde bude opäť potrebný zistiť určitý reťazec znakov, v tomto prípade bude potrebné overiť, či sa v texte nachádza reťazec **<a href = " ">**, ktorý označuje hypertextový odkaz. V súbore sa môžu vyskytovať desiatky takýchto odkazov, či už sa bude jednať o odkazy smerujúce na stránku, odkaz na obrázok, popr. o odkazy na väčší počet stránok, bude potrebné prispôsobiť program tomu, aby nastavil číslo 1 pri adrese, z ktorej email príde. Týmto bude možné zistiť, koľko emailov z celkového počtu emailov obsahovalo hypertextové odkazy. V prípade, že by z jednej adresy prišlo emailov viac, bude v poli, ktoré bude takýto výskyt počítať, presný počet súborov s odkazmi. Následne sa bude taktiež zisťovať, koľko odkazov bolo v emailoch celkovo, aby bolo možné štatisticky spočítať priemerné množstvo odkazov v jednom súbore.

Takéto vyhľadávanie odkazov však nemusí znamenať, že nájdený súbor s odkazom skutočne odkazuje na podvodnú stránku, teda že sa jedná o pharming alebo phishing. Vykonanie kompletnej analýzy obsahu všetkých emailových súborov by bolo zložité, preto bude potrebné po zistení celkového počtu emailov s odkazmi ručne analyzovať určité množstvo emailov, aby sa približne dalo určiť, či sa v emailoch nachádzajú aj podvodné stránky alebo nie, popr. zistiť, či sa v emailoch nachádzajú odkazy na reklamné stránky, alebo na odkazy, kde je možné sa odhlásiť z odberu noviniek. Emailový balík, ktorý bol pre túto kategorizáciu použitý je však pár mesiacov starý, môže sa teda stať, že odkazy, ktoré boli pred pár mesiacmi funkčné už budú zrušené, teda stránka sa nemusí nájsť, popr. môže ísť o doménu na predaj.

Konkrétny reťazec, ktorý sa bude v emailových súboroch hľadať, je možné vidieť na obrázku 7:

```
<!DOCTYPE html><html><head>
<meta http-equiv=3D"Content-Type" content=3D"text/html;
charset=3Dutf-8"></=
head><body>=0D
<div align=3D"center">=0D
I v=C3=A1=C5=A1 mil=C3=BD hlasit=C4=9B chr=C3=A1pe? S regul=C3
=A1torem d=C3=
=BDch=C3=A1n=C3=AD ho m=C5=AF=C5=BEete uti=C5=A1it<br><a href=
3D"http://kxt=
h.mudrahospital.com/" style=3D"font-style:italic; text-
align:left; "><img s=
tyle=3D"text-indent:auto; height:auto; padding-bottom:3px;
padding-right:3p=
x; " src=3D"http://hq.mudrahospital.com/00.jpg" alt=3D"Na
hlasit=C3=BD sp=
=C3=A1nek: regul=C3=A1tor d=C3=BDch=C3=A1n=C3=AD, l=C3=A9pe si
s n=C3=ADm o=
dpo=C4=8Dine=C5=A1"></a>=0D
<br><a style=3D"padding-left:2px; border-bottom-color:#ffffff;
border-botto=
m:solid 1px #ffffff; " href=
3D"http://kxth.mudrahospital.com/">=C5=98e=C5=
=A1en=C3=AD na chr=C3=A1p=C3=A1n=C3=AD - poznej m=C5=AFj p=C5=
99=C3=ADb=C4=
=9Bh pln=C3=BD zvrat=C5=AF, =C5=99e=C5=A1en=C3=AD
existuje</a>=0D
<br><br><br><br>Kv=C5=AFli man=C5=BEelovu chr=C3=A1p=C3=A1n=C3
=ADm nem=C5=
=AF=C5=BEete sp=C3=A1t? Uti=C5=A1te ho novou pom=C5=AFckou
proti chr=C3=A1p=
=C3=A1n=C3=AD<br><br><a style=3D"font-size:12px; background-
color:#ffffff; =
margin-top:auto; margin:3px; border-bottom-width:2px; border-
left-color:#cc=
0000; " href=3D"http://mudrahospital.com/ub.php?we=
3Dknbup64124070bxwpw2zt0=
8q0gw4b9rthmpi5t3">odhl=C3=A1sit</a></div><br>Ty je=C5=A1t=C4=
9B chr=C3=A1p=
e=C5=A1? S regul=C3=A1torem d=C3=BDch=C3=A1n=C3=AD hluk za
p=C3=A1r dn=C3=
=AD p=C5=99estane=0D
<img src=3D"http://mudrahospital.com/ob.php?g1=
3Dknbup64124070bxwpw2zt08q0g=
w4b9rthmpi5t3">=0D
</body>=0D
</html>=
```

Obrázok 7 – Emailový súbor obsahujúci odkaz

V prípade nájdenia takéhoto odkazu sa k adrese, z ktorej tento email prichádzal, zapíše informácia o tom, že obsahoval odkaz a následne sa zistí, koľko takýchto odkazov v ňom skutočne bolo.

2.4 Vydieračské emaily

Vydieračské emaily sa stávajú čoraz viac populárnejšími, pričom útočníci vo väčšine prípadov vydieračských emailov žiadajú peniaze práve v mene bitcoin. Dôvodom je fakt, že nie je jednoduché dopátrať to, komu bitcoinová peňaženka patrí. Cieľom v tejto časti bude zistiť to, či sa vôbec vydieračské emaily v poskytnutom balíku nachádzajú. K tomu budú

použité kľúčové slová, ktoré sa v obsahu emailu budú hľadať a tým bude možné takýto email nájsť. Problémom pri takomto hľadaní môže byť práve to, že tieto emaily môžu byť poslané v akomkoľvek jazyku a môžu mať tiež akýkoľvek obsah. Jedinou istotou v prípade takéhoto typu emailu je to, že vždy sa v ňom bude vyskytovať jedno z troch kľúčových slov, teda sa tam bude nachádzať slovo **bitcoin**, **BTC** alebo **wallet**, v preklade peňaženka. Podľa týchto troch kľúčových slov sa navrhnuté skripty budú snažiť zistiť, či sa o vydieračský bitcoinový email skutočne jedná alebo nie.

V prípade, že sa nájde nejaký vydieračský email, bude zapísaný počet takýchto súborov pri konkrétnej adrese číslom a taktiež bude zapísaný názov súboru, v ktorom sa email s vydieračským obsahom nachádza. Tieto emaily budú následne ručne analyzované, čím sa zistí niekoľko podstatných informácií ako napr. jazyk, v ktorom boli tieto emaily písané, aké množstvo financií a v akej mene ich žiada a pod. Taktiež bude potrebné zanalyzovať odkiaľ tento email prichádza, následne bude adresa preverená službami pre kontrolu IP adries, aby sa zistilo, či sa adresa nachádza na nejakom blackliste. Peňaženka, ktorá bude v obsahu emailu, sa pomocou bitcoin blockchainu skontroluje, aby sa zistilo, či je táto peňaženka finálna alebo sa bitcoiny z nej preposielajú na inú peňaženku. Týmto sa docieli širší prehľad o funkčnosti tohto systému, akým štýlom útočníci ľudí vydierajú a pod. Príklad takéhoto emailu je možné vidieť na obrázku 8:

```
Pro tento okam&#382;ik je v&#225;&#353; emailov&#253; &#250;&#
269;et =
napaden (viz , nyn&#237; m&#225;m p&#345;&#237;stup k va&#353;im
=
&#250;&#269;t&#367;m)..
Stahoval jsem v&#353;echny d&#367;v&#283;rn&#233; informace z =
va&#353;eho syst&#233;mu a dostal jsem dal&#353;&#237; d&#
367;kazy.
Nejzaj&#237;mav&#283;j&#353;&#237;m okam&#382;ikem, kter&#253;
jsem =
objevil, jsou videoz&#225;znamy o v&#225;s masturbuj&#237;c&#
237;.

Zve&#345;ejnil jsem virus na pornografick&#233;m webu, a pak
jste jej =
nainstalovali do sv&#233;ho opera&#269;n&#237;ho syst&#233;mu.
Po klepnut&#237; na tla&#269;&#237;tko P&#345;ehr&#225;t na
porno video, =
v tom okam&#382;iku byl m&#367;j trojan sta&#382;en do va&#
353;eho =
za&#345;&#237;zen&#237;.
Po instalaci v&#225;m p&#345;edn&#237; fotoapar&#225;t =
nat&#225;&#269;&#237; video poka&#382;d&#233;, kdy&#382;
masturbujete, =
software se synchronizuje s vybran&#253;m videem.

Prozat&#237;m software z&#237;skal v&#353;echny va&#353;e
kontaktn&#237; =
informace ze soci&#225;ln&#237;ch s&#237;t&#237; a e-mailov&#
253;ch =
adres.
Pokud pot&#345;ebujete smazat v&#353;echny =
shrom&#225;&#382;d&#283;n&#233; &#250;daje, po&#353;lete mi $250
v BTC =
(krypto m&#283;n&#283;).

Toto je moje Bitcoin pen&#283;&#382;enka: =
1GL9JtXPRTPetxgiJ8UcgrEECp12spD4tt=20
M&#225;te 48 hodin po p&#345;e&#269;ten&#237; tohoto dopisu.

Po transakci vyma&#382;u v&#353;echna data.
Jinak pos&#237;l&#225;m video se va&#353;&#237;m &#382;ert&#
237;ky =
v&#353;em va&#353;im koleg&#367;m a p&#345;&#225;tel&#367;m!!

V budoucnosti bu&#271;te opatrn&#283;j&#353;&#237;
Nav&#353;tivte pros&#237;m pouze zabezpe&#269;en&#233; weby!
Sbohem!
```

Obrázok 8 – Príklad vydieračského bitcoinového emailu

Z obrázku 8 je zrejmé, že aj keď je text ťažko čitateľný a význam by sa v ňom hľadal taktiež ťažko, dve z kľúčových slov sa v obsahu nachádzajú, preto bude možné ho správne zaradiť do kategórie vydieračských emailov. Takto nájdené emaily budú aj s číslom súboru zapísané do výslednej tabuľky údajov, vďaka ktorej bude možné presne zistiť to, o ktorý súbor sa jednalo a tým bude možné ho podrobiť bližšej analýze.

II. PRAKTICKÁ ČÁST

3 SKRIPTY

Z návrhu vypracovania boli vytvorené skripty, ktoré veľké množstvo spamových emailov kategorizujú presne tak, ako to bolo v návrhu popísané, či už sa jedná o zistenie IP adresy a krajiny, zistenie príloh alebo o odhalenie vydieračského emailu. Tieto skripty boli vytvorené v programovacom jazyku Python, ktorý bol pre vyhľadávanie kľúčových slov a reťazcov znakov najviac vhodný.

Skripty samotné sa skladajú z 2 súborov, ktoré nesú názvy main.py a ipaddress.py. V ipaddress.py je zahrnutá inicializácia premenných triedy, samotná trieda, vyhľadávanie a limity na čakanie v prípade spracovania určitého počtu požiadavkov, čím bude možné sa vyhnúť zablokovaniu IP adresy na stránke ip-api.com, z ktorej sa API využíva a kde dochádza k preverovaniu IP adries z emailov. Main.py obsahuje všetok zvyšný potrebný kód, či už sa jedná o vytvorenie .csv súboru, o samotné triedenie alebo o zápis spracovaných dát do výstupného súboru.

3.1 IPaddress.py

```
import gc
import json
import time
```

Na začiatku sa naimportujú všetky potrebné použité knižnice, ktoré sú použité v rámci zdrojového kódu. Použitie týchto knižníc veľmi uľahčilo následnú prácu, pretože nebolo potrebné vymýšľať niečo, čo už vymyslené bolo.

```
from urllib.request import urlopen
```

V prípade importu knižnice urlopen sa jedná o knižnicu pre spracovanie http požiadavku, čo sa používa k získaniu údajov a detailov k nájdeným IP adresám.

```
request_counter = 0
```

Keďže obmedzenie na hľadanie adries, o ktorom sa v návrhu hovorilo je 150 adries za jednu minútu, bolo potrebné inicializovať túto premennú pre počítanie celkového počtu spracovaných adries.

```
# Ip Address
class ip_address_t:

    # Constructor
    def __init__(self, address):

        self.address = address
```

Bolo potrebné vytvoriť triedu, ktorá bude uchovávať informácie o unikátnych IP adresách, teda aby sa nenachádzala v zozname jedna adresa viac ako jedenkrát. Tiež slúži na dohľadávanie informácii k týmto adresám. V konštruktore dôjde k uloženiu IP adresy do premennej vo vnútri triedy.

```
# Lookup
def lookup(self):

    global request_counter

    # Skip if the lookup already occurred.
    if self.country != "" or self.country_code != "":
        return
```

V časti lookup sa nachádza metóda pre bližšie dohľadanie informácii IP adresy a tiež je tu prístup ku globálnej premennej na predídenie banu. Aby sa predišlo tomu, aby sa tie isté informácie hľadali viackrát a tým by sa zvyšovali požiadavky na server, je tu podmienka, ktorá ukončí metódu ak už boli informácie k tejto IP adrese raz nájdené.

```
# Wait if the request counter exceeds the maximum value.
if request_counter >= 145:
    print("Waiting for next request and freeing memory.")
    request_counter = 0
    time.sleep(62)
    gc.collect()

request_counter += 1
```

V prípade, že limit 145 emailov sa naplní, je uvoľnená pamäť a následne sa čaká 62 sekúnd kvôli predídeniu blokácii IP na stránke ip-api.com. Táto stránka má limit 150 požiadaviek za jednu minútu.

```
try:
    data = json.loads(urlopen("http://www.ip-api.com/json/" +
self.address).read())

    self.country = data["country"]
    self.country_code = data["countryCode"]

except:
    return
```

V časti kódu try sa vyvolá požiadavka na server ip-api. Výsledkom tejto požiadavky sú výsledné dáta vo formáte JSON, ktoré obsahujú všetky čiastkové informácie k danej IP adrese. Tu sa nachádzajú úplne všetky údaje, teda krajina, kód krajiny, mesto, kraj, mnou navrhnutý program ale ukladá do premenných len krajinu a jej kód, pretože nič viac nie je potrebné. V prípade, že by došlo k nejakej vážnej chybe, sa hľadanie ukončí.

Následne sú inicializované premenné triedy, ktoré sú využívané v programe main.py. Konkrétne sa jedná o inicializáciu premenných:

```
address = ""
count = 0
country = ""
country_code = ""

bitcoins = 0
bitcoin_filenames = ""
http_count = 0
href_count = 0

extension_counts = {}
```

Inicializované premenné slúžia k uloženiu údajov o IP adrese, počet emailov z jednej adresy, kód krajiny a krajinu, ale aj informácie o bitcoinoch, hypertextových odkazoch a o príponách súborov.

3.2 Main.py

```
import glob
import os
import re
import sys
import tempfile

from IpAddress import ip_address_t
from pathlib import Path
```

Na začiatku programového súboru sú opäť importované všetky potrebné knižnice a funkcie, ktoré sa budú využívať v rámci celého kódu. Najviac pomocné sú práve knižnice pre prácu so súbormi, ich otváranie, čítanie a zapisovanie.

```
# Statistics
extensions = [ "zip", "exe", "vsb", "jar", "doc", "docx", "pdf", "xml",
"ixml", "jpg", "jpeg", "png" ]
bitcoin_addresses = [ "zacek@utb.cz", "zacek@fai.utb.cz",
"ekonference@utb.cz", "e-konference@utb.cz" ]
```

Pod štatistikami sa rozumejú polia, v ktorých sú uložené všetky potrebné údaje pre hľadania. Jeden stĺpec v .csv súbore odpovedá práve jednej položke z pola extensions. V poli extensions sú uložené prípony súborov, ktoré sa vyhľadávajú, kde boli vybrané prípony, ktoré sa môžu, ale nemusia vyskytnúť najčastejšie. V poli bitcoin_addresses sú uložené emaily, ktoré sa prehľadávajú pri hľadaní vydieračských emailov. Tieto emaily je taktiež možné pridať alebo zmeniť v prípade potreby alebo za účelom rozšírenia.

```
ip_addresses = []
```

V premennej ip_addresses je zoznam dosiaľ všetkých nájdených IP adries.

```
# Add IP Address to the global list.
def add_ip_address(address, extension_counts, bitcoin_filename,
http_count, href_count):

    target = None

    # Increase counter if the address already exists in the list.
    for i in ip_addresses:
        if i.address == address:
            target = i
            break
```

Následne bola zadefinovaná funkcia pre pridávanie buďto novej IP adresy do zoznamu, alebo pre pričítanie jednotky k už nejakej nájdenej IP adrese v prípade, že už existuje. V prípade, že IP adresa nájdená nebola, sa vytvorí adresa nová. Do premennej target sa budú ukladať zadané hodnoty. Cyklus for prehľadáva všetky stávajúce IP adresy, čím zistí, či sa adresa z premennej ip_address už nevyskytuje. Ak áno, je uložená do premennej target.

```
# Create new address if it wasn't found.
if not target:
    target = ip_address_t(address)
    target.extension_counts = {}
    for i in extensions:
        target.extension_counts[i] = 0

    target.lookup()
    ip_addresses.append(target)
```

V prípade, že sa v rámci predchádzajúceho cyklusu target nezmenil, vytvorí sa nová adresa a je pridaná na koniec zoznamu IP adries v .csv súbore. Target.lookup() následne zistí ďalšie potrebné informácie ohľadom IP adresy a samotný append ju do zoznamu pridá.

```
for i in extensions:
    target.extension_counts[i] += extension_counts[i]
target.count += 1
```

V cykle sa k cieľovej IP pričíta počet nájdených súborov. Aby sa adresa samotná nevyskytovala vo výstupe z programu niekoľko krát, bude tam len raz, pričom jej počet bude nastavený práve na množstvo daných výskytov.

```
# Bitcoins
target.bitcoins += 1 if bitcoin_filename != "" else 0
target.http_count += http_count
target.href_count += href_count

if bitcoin_filename != "":
    if target.bitcoin_filenames != "":
        target.bitcoin_filenames += ","

    target.bitcoin_filenames += bitcoin_filename
return target
```

Ak sa v súbore našiel bitcoin, k IP adrese, z ktorej prišiel, sa k počtu bitcoinov pričíta 1, ak premenná bitcoin_filename nie je prázdna. V prípade, že sa v súbore nachádzajú nejaké hypertextové odkazy, sú taktiež pričítané k príslušným premenným. Podmienka if sa v kóde vyskytuje preto, že môže nastať situácia, kedy z jednej IP adresy prišlo viac takých bitcoinových emailov. Aby sa zabránilo prepísaniu názvu už nájdeného súboru, vloží sa čiarka ako oddeľovač a za ňu je vložený názov ďalšieho súboru. Takto sa za seba skladajú bitcoinové emaily v prípade, že by ich skutočne bolo vyššie množstvo. Vráti sa vždy buď novo vytvorená IP adresa alebo niektorá z už vytvorených adries.

```
# Parse file
def parse_file(filename):

    global extension_counts

    print("Parsing file \"" + filename + "\'.")
```

Následne bola vytvorená funkcia pre spracovanie jedného .emlx emailového súboru a taktiež bol pridelený prístup ku globálnej premennej. Aby bolo možné vidieť, ktorý súbor sa momentálne spracováva, bol pridaný výpis na konzolu s aktuálnym názvom súboru.

```
try:
    data = open(filename, "r", errors = 'ignore').read()

    # Find all IP addresses inside the file.
    results = re.findall("Received: .*\[([0-9]+\.[0-9]+\.[0-9]+\.[0-
9]+)\].*\n", data)
    result_count = len(results)
```

V časti kódu try dochádza k otvoreniu súboru a načítaniu celého jeho obsahu do premennej dáta. Ak sú nejaké chyby v kódovaní súboru, bude ich ignorovať. Následne sa pomocou regex-u budú nachádzať adresy v celom obsahu súboru. Nachádza len tie, pred ktorými je reťazec **Received:** a ktoré sa nachádzajú vo vnútri hranatých zátvoriek. Týmto sa hľadajú IP adresy priamo len v hlavičke súboru. Takáto hlavička má presne definovaný formát. Následne premenná result_count uloží počet nájdených adries.

```
# The last IP address is the correct one unless it is localhost.
address = results[result_count - 1]

if address == "127.0.0.1" and result_count > 1:
    address = results[result_count - 2]

print("Found IP \"" + address + "\".")
```

Posledná nájdená IP adresa je tá správna ktorú je potrebné vybrať. Môže sa ale stať, že posledná adresa by bola 127.0.0.1, čo značí localhost, takže v takomto prípade sa vyberie adresa predposledná. Taktiež je na konzolu nastavený výpis práve nájdenej IP adresy.

```
        # Detect whether or not bitcoin wallet is included in the email.
        sender = re.findall("From: .*\<(.*)\>", data)
#         receiver = re.findall("To: .*\<(.*)\>", data)
```

Podľa definovaného .emlx formátu sa hľadá odosielateľ. Vie sa, že pred samotným emailom odosielateľa musí byť reťazec **From:** a že samotný email je v hranatých zátvorkách. Pôvodne bolo takto nastavené aj hľadanie príjemcu, kde sa tieto 2 emaily následne porovnávali či sú rovnaké, čo mohlo značiť že sa jedná o vydieračský email. Toto riešenie však nebolo postačujúce.

```
bitcoin_filename = ""
if len(sender) > 0 and len(re.findall("btc|bitcoin|wallet", data,
re.IGNORECASE)) > 0:
    for i in bitcoin_addresses:
        if sender[0] == i:
            bitcoin_filename = Path(filename).stem
            break
```

V tejto časti kódu sa kontroluje, či súbor obsahuje bitcoinovú peňaženku. Hľadá sa to tak, že sa vychádza z počtu nájdených kľúčových slov, ktoré sú **btc**, **bitcoin** a **wallet**. Ak je nájdené aspoň jedno takéto slovíčko a zároveň nie je políčko odosielateľa prázdne, kód postúpi k porovnaniu odosielateľa s predom definovanými emailovými adresami. Ak sa nájde zhodný email, súbor je označený za bitcoin, teda vydieračský email a do premennej bitcoin_filename uloží názov .emlx súboru bez koncovky. V prípade že sa takýto email nájde, cyklus je ukončený.

```
# Count attachments.
extension_counts = {}
for i in extensions:
    extension_counts[i] = len(re.findall("[\s;]name\s*=\s*\".*\.(" + i +
")\"", data, re.IGNORECASE))
```

Inicializuje sa pomocné pole pre uloženie počtu výskytu koncoviek súborov a následne pre každú jednu koncovku v globálnom poli extensions sa vykoná jej vyhľadaniu v obsahu súboru. Formát vyhľadávania je **name = "názov súboru.koncovka súboru"**. Následne sa k prvku i pomocnej premennej pričíta celkový počet nálezov.

```
# Count http occurrences.
href_count = len(re.findall("<\s*a.+href\s*=", data, re.IGNORECASE))
http_count = 1 if len(re.findall("<\s*a.+href\s*=", data, re.IGNORECASE))
> 0 else 0

add_ip_address(address, extension_counts, bitcoin_filename, http_count,
href_count)
```

V tejto časti kódu sa vyhľadáva, koľkokrát sa vyskytuje referencia na nejakú webovú stránku v súbore. Formát vyhľadávania je, že v lomených zátvorkách sa musí nachádzať **<a href="**

“>, pričom medzi slovami **a** a **href** môže byť napísané čokoľvek. Premenná http_count kontroluje, či sa nejaká referencia v súbore nachádza. Ak áno, zapíše sa logická 1, ak nie, zapíše sa logická 0. Premenná href_count naopak zapisuje celkový výskyt referencií v súbore, nie len či sa referencia vyskytuje. Následne sa na koniec súboru pridá zistená adresa.

```
except:
    print("Error! Ignoring file.")
```

Taktiež sa môže stať, že počas hľadania dôjde k akejkoľvek chybe, napr. pri čítaní súboru alebo pri jeho spracovávaní. V takomto prípade sa len vypíše chybová hláška na konzolu a súbor sa preskočí, zabráni sa tak ukončeniu programu.

```
# Write output file
def write_output(filename):

    try:
        file = open(filename, "w")

    except:
        file = tempfile.NamedTemporaryFile(mode = "w", delete = False)
        print("Unable to open " + filename + ". Saving to temp " +
file.name)
```

Následne bola vytvorená funkcia pre zapísanie výsledného .csv súboru. V časti try sa program pokúsi súbor otvoriť, aby do neho mohlo byť zapisované. V prípade, že by súbor otvoriť nešiel, napr. kvôli tomu že už je otvorený, tak sa vytvorí dočasný súbor v zložke temp používateľa, kde sa obsah zapíše.

```
# Header
file.write("Address;Country;Country Code;Count;")

for i in extensions:
    file.write(i + ";")

file.write("Bitcoins;Bitcoin Filenames;Http;Href\n")
```

V časti Header je vytvorená hlavička CSV súboru, kde sa jednotlivé stĺpce oddeľujú bodkočiarkou miesto čiarky kvôli podpore programu MS Excel.

```
for i in ip_addresses:
    file.write(i.address + ";" + i.country + ";" + i.country_code + ";" +
str(i.count) + ";")
    for j in extensions:
        file.write(str(i.extension_counts[j]) + ";")

    file.write(str(i.bitcoins) + ";" + i.bitcoin_filenames + ";" +
str(i.http_count) + ";" + str(i.href_count) + "\n")
```

Následne sa v cykloch hlavička vyplní získanými údajmi a zapíšu sa koncovky súborov, ktoré sú oddelené bodkočiarkou. Takto sú vyplnené všetky dáta v hlavičke.

```
# bachelor.py rootDirectory outputFile
if len(sys.argv) < 3:
    exit(-1)

# Parse all files inside the root directory.
files = glob.iglob(sys.argv[1] + "/*.emlx")
file_counter = 0
for i in files:
    file_counter += 1
    print("File " + str(file_counter) + ":")
    parse_file(i)
```

Zistí sa root zložka výsledného a prehľadáva celú zložku, aby v nej našiel súbory. Následne file_counter počíta, koľký súbor sa práve spracováva a vypisuje na konzolu pomocné informácie o súboroch.

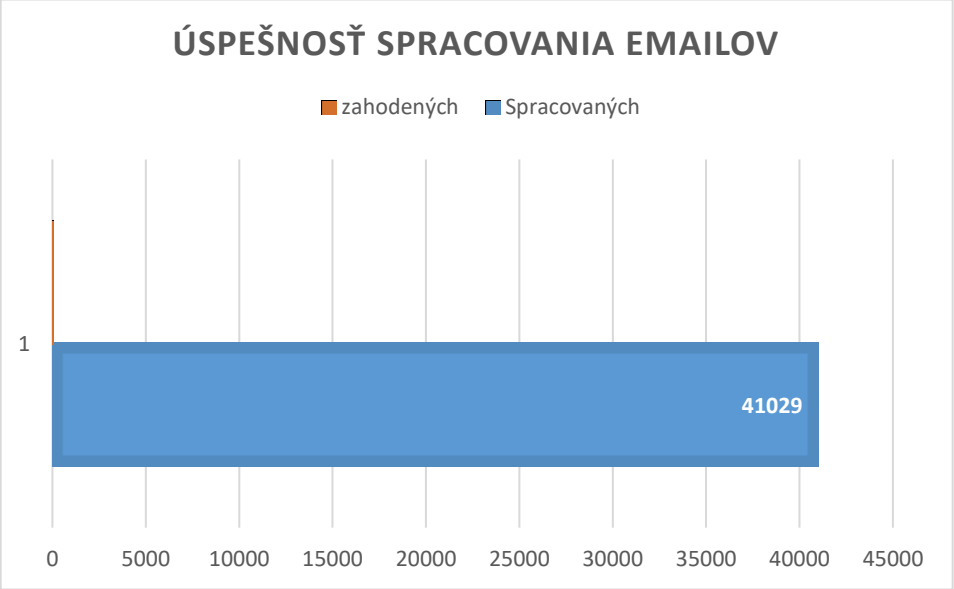
```
# Write the results to the output file.
write_output(sys.argv[2])

print()
print("Done! Saved to: " + sys.argv[2])
```

Na konci celého programu je funkcia, ktorá spôsobí, že všetko čo v programe prebehlo, sa zapíše až po spracovaní súborov. Následne na konzolu už len vypíše informáciu, že kategorizácia emailov je hotová a napíše lokáciu, kam bol výsledný súbor s výstupmi uložený.

4 ŠTATISTIKA

Skripty, ktoré boli vypracované v prechádzajúcej časti bakalárskej práce, boli použité na balík emailov, resp. emailových súborov vo formáte .emlx, ktoré boli pre túto bakalársku prácu poskytnuté vedúcim práce. Veľký dôraz pri vytváraní skriptov sa kládol na to, aby boli čo najpresnejšie a aby čítací pomer bol čo najlepší. Keďže z celkového počtu emailov 41072 bolo úspešne spracovaných 41029, dá sa povedať, že čítací pomer je dostatočne presný. Úspešnosť graficky je možné vidieť na obrázku 9:



Obrázok 9 – Graf úspešnosti spracovania emailov

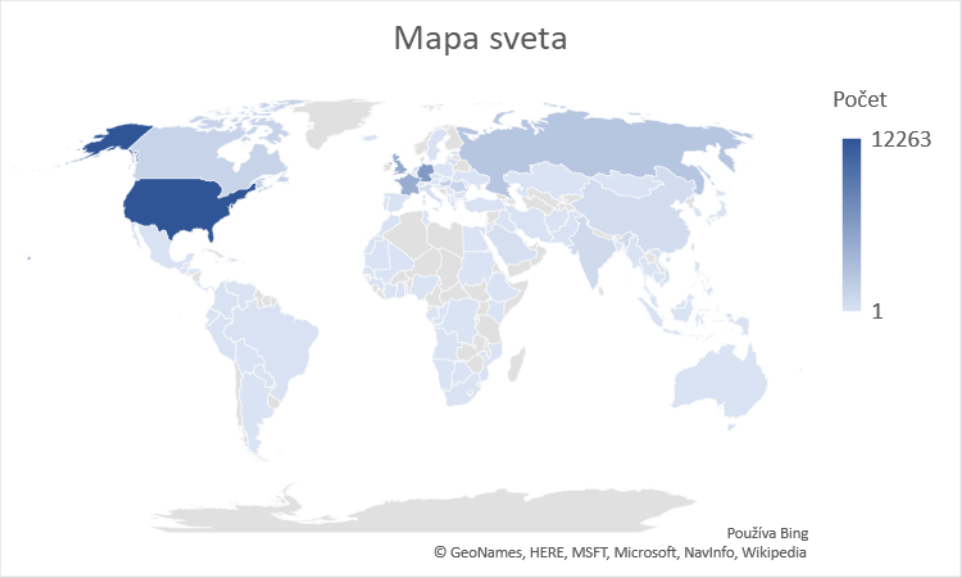
Ako je možné vidieť na obrázku 9, úspešnosť sa pohybuje približne na hranici 99,895%, čo je vyhovujúci výsledok.

Dáta, ktoré boli z týchto emailových súborov získané, boli úspešne zapísané do .csv súboru, kde boli následne ďalej spracované pre použitie do štatistiky. V nasledujúcej kapitole budú prehľady, grafy a štatistiky o týchto emailoch z viacerých pohľadov – či už sa bude jednať o prehľad odkiaľ emaily pochádzali, ktoré krajiny boli do rozosielania zapojené najviac, koľko z nich obsahovalo súbor, ktoré mali vydieračský obsah alebo ktoré mali aj nejaký odkaz.

Niektoré prehľady budú taktiež porovnané so svetovými štatistikami, čím bude možné vidieť to, ako ovplyvňuje žitie v Českej republike príjem spamových emailov oproti svetovým krajinám. Štatistiky sa nemusia plne zhodovať s tými, ktoré je možné nájsť na internete.

4.1 Frekventovanosť krajín a najväčší odosielatelia spamu

Keďže z celkového počtu 41072 emailov bolo úspešne spracovaných 41029, z týchto emailov bola vytvorená štatistika, teda mapa sveta ukazujúca to, ktoré krajiny boli do rozosielania spamových emailov zapojené. Výsledky je možné vidieť na obrázku 10, kde krajiny, ktoré do odosielania takýchto emailov zapojené neboli, sú zobrazené farbou šedou, krajiny zapojené len čiastočne svetlomodrou farbou a krajiny, ktoré sa zapojili najviac, sú označené tmavomodrou farbou.



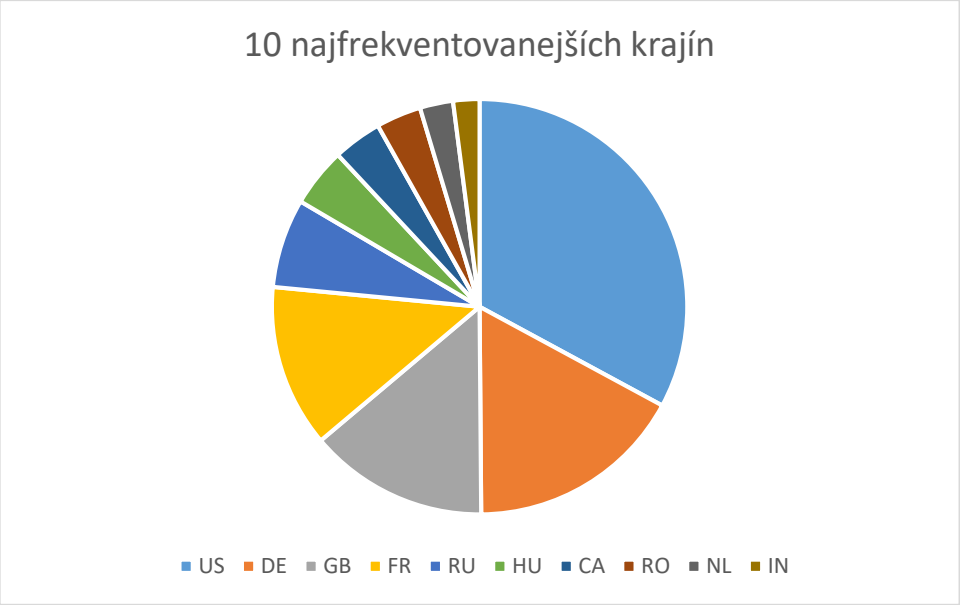
Obrázok 10 – Mapa sveta so zapojenými krajinami

Do odosielania spamových emailov sa zapojilo celkovo 105 krajín z celého sveta, čo je z celkového počtu 195 krajín sveta takmer 54%. Toto číslo je dostatočne veľké, v prípade, že by boli analyzované emaily z väčšej databázy emailov namiesto poskytnutého balíku, mohlo by byť toto číslo ešte väčšie.

Z mapy sveta s označenými krajinami je možné vidieť, že najväčším odosielateľom spamových emailov sú práve Spojené štáty americké. Z 41029 išlo práve 12263 z USA, čo tvorí obrovskú časť z týchto emailov, percentuálne takmer 30%. Druhé v poradí bolo Nemecko, ktoré poslalo 6333 emailov, teda približne 15,4% emailov a na tretej priečke sa umiestnilo Spojené kráľovstvo, ktoré poslalo 11,5%, teda 5212 emailov. Ďalšie krajiny, ktoré sa hojne zapojovali do rozosielania spamových emailov boli napr. Francúzsko, Rusko alebo aj Slovensku susedné Maďarsko, odkiaľ prišlo 1711 emailov. Pre porovnanie s väčšími štátmi, Slovenská republika poslala len 4 spamové emaily a Česká republika poslala 24 spamových emailov, čo je dokopy len 0,06% zo všetkých poslaných emailov.

Z toho vyplýva, že z našich krajín sa posiela najmenej nevyžiadanej pošty. Pri porovnaní týchto dvoch krajín dokopy, či už sa jedná o rozlohu krajiny alebo o počet obyvateľov, veľmi vybočujú z priemeru, ktorý je v prípade analýzy poskytnutého balíku 566,4 emailov z každej krajiny.

10 krajín, ktoré posielali hromadne nevyžiadanú poštu najfrekventovanejšie je možné vidieť na obrázku 11:



Obrázok 11 – 10 najfrekventovanejších krajín odosielania spamových emailov

Štatistika, ktorú sa podarilo zistiť z balíku, je nie úplne zhodná so svetovou štatistikou z roku 2018, podľa ktorej je najväčším odosielateľom nevyžiadanej pošty práve Čína. Tá práve v roku 2018 rozoslala približne 11,69% z celkového počtu spamových emailov a na druhom mieste sa umiestnili Spojené štáty americké s 9,04%. Tretím najväčším odosielateľom je podľa štatistík Nemecko, ktoré poslalo 7,17% z celkového počtu spamu. [22]

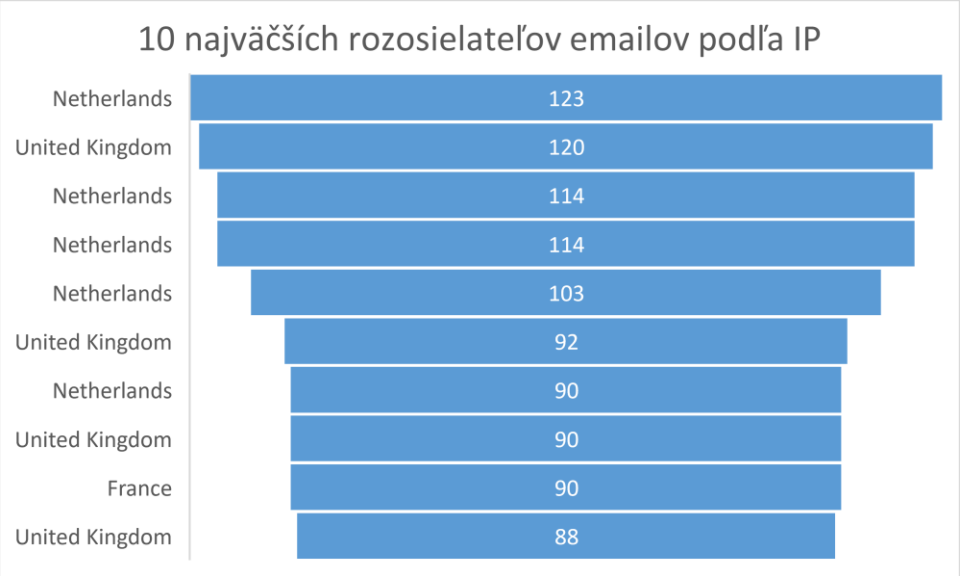
V štatistike získanej z tohto balíku sa Čína nedostala sa ani do 10 najfrekventovanejších krajín, pričom z nej prišlo len 573 emailov. V prípade, že by Čína nebola zaradená do štatistiky, by sa štatistika zhodovala viac s tou svetovou. Spôsobené to môže byť tým, že Česká republika sa nachádza práve v srdci Európy a útočníci a odosielatelia spamového emailu nevidia v tejto krajine príliš veľký potenciál.

Podrobnejší prehľad o počte spamových emailov zo známych štátov sveta je uvedený v tabuľke 1:

Tabuľka 1 – Početnosť emailov zo známych štátov sveta

Známe štáty a početnosť emailov z nich		
Krajina	**Kód krajiny**	**Počet emailov**
Spojené štáty americké	US	12263
Nemecko	DE	6333
Spojené kráľovstvo	GB	5212
Francúzsko	FR	4723
Rusko	RU	2587
Maďarsko	HU	1711
Kanada	CA	1419
Rumunsko	RO	1309
Holandsko	NL	963
India	IN	764
Čina	CN	573
Saudská Arábia	SA	337
Taliansko	IT	336
Vietnam	VN	280
Švédsko	SE	117
Irán	IR	89
Mexiko	MX	66
Brazília	BR	61
Pakistan	PK	54
Bangladéš	BD	32
Hongkong	HK	26
Ukrajina	UA	25
Poľsko	PL	24
Česká republika	CZ	24
Južná Kórea	KR	20
Španielsko	ES	13
Portugalsko	PT	12
Izrael	IL	12
Grécko	GR	10
Irak	IQ	8
Japonsko	JP	7
Chorvátsko	HR	4
Slovensko	SK	4
Rakúsko	AT	3

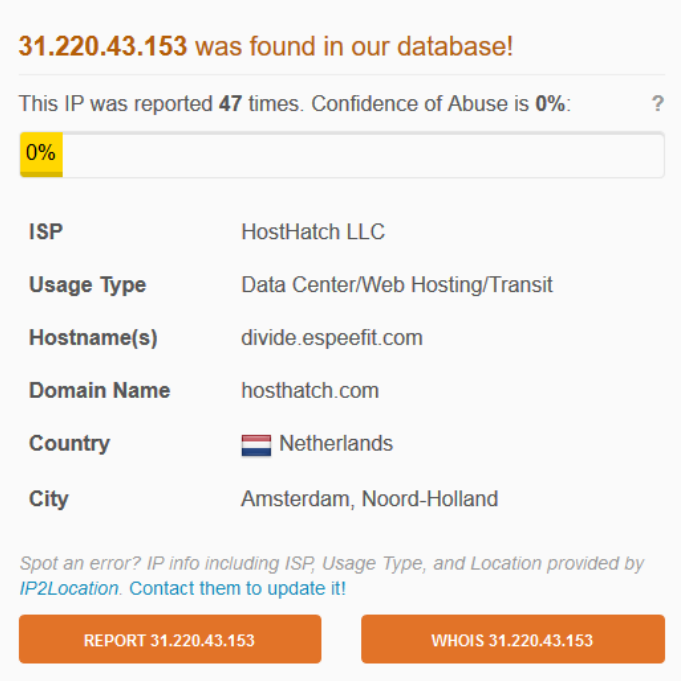
V zozname bolo pomocou príkazov v MS Excel vyhľadaných 10 najčastejších IP adries, aby sa zistilo, koľko emailov išlo najviac z jednej adresy, odkiaľ títo odosielatelia boli a či sa tieto adresy nachádzali medzi hlásenými na stránkach, ktoré kontrolujú, či sú adresy blokované antispamovou službou a pod. Z 10 najčastejších IP adries bol vytvorený graf, ktorý je možné vidieť na obr. 12:



Obrázok 12 – 10 najväčších rozosielateľov emailov podľa IP adresy

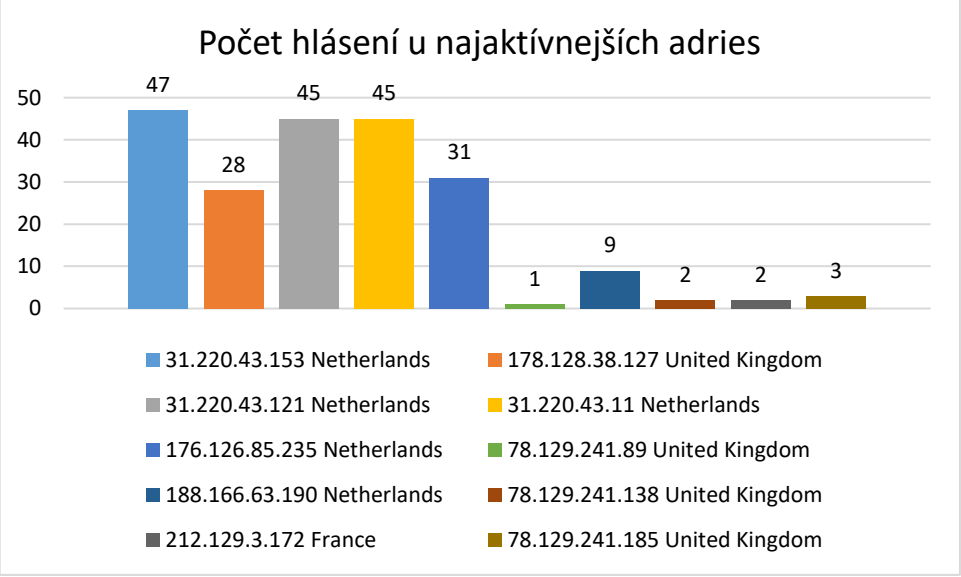
Z obrázku jasne vyplýva, že najviac emailov prišlo práve z IP, ktorá sa nachádzala v Holandsku, no taktiež to, že práve spameri pochádzajúci z Holandska patria medzi tých najaktívnejších. Aj keď z Holandska samotného neprišlo najviac emailov, v prepočte na jedného spamera je to asi najaktívnejšia krajina. Medzi najväčšími odosielateľmi sa nachádzalo aj Spojené kráľovstvo, ktoré z celkového počtu emailov poslalo 11,5% emailov, čím sa stalo 3. najväčším rozosielateľom emailov. V zozname 10 najväčších odosielateľov sa objavilo aj Francúzsko.

Pomocou stránky AbuseIPDB boli všetky tieto IP adresy skontrolované, aby sa zistilo, či sa nachádzajú na blacklistoch, teda na čiernych zoznamoch služieb ktoré kontrolujú adresy. Výsledkom kontroly bol počet nahlásení, ktoré každá adresa mala, teda koľko užívateľov túto adresu označilo za škodlivú alebo inak nevhodnú. Príklad zisťovania počtu hlásení pomocou stránky AbuseIPDB je zobrazený na obrázku 13:



Obrázok 13 – Výstup zo stránky AbuseIPDB

Vďaka takýmto hláseniam, ak ich je teda dostatočné množstvo, môže byť táto adresa preposlaná ďalším osobám, ktoré spravujú blacklisty, a tak ju pridajú do svojej databázy. Celkový prehľad počtu hlásení, ktoré boli získané zo stránky AbuseIPDB, je možné vidieť na obrázku 14:



Obrázok 14 – Počet hlásení u najaktívnejších adries

Z obrázku 14 je zrejmé, že práve IP adresy, ktoré pochádzajú z Holandska boli nahlasované najčastejšie. Zatiaľ ale neboli považované za natoľko škodlivé, aby ich zablokovali alebo

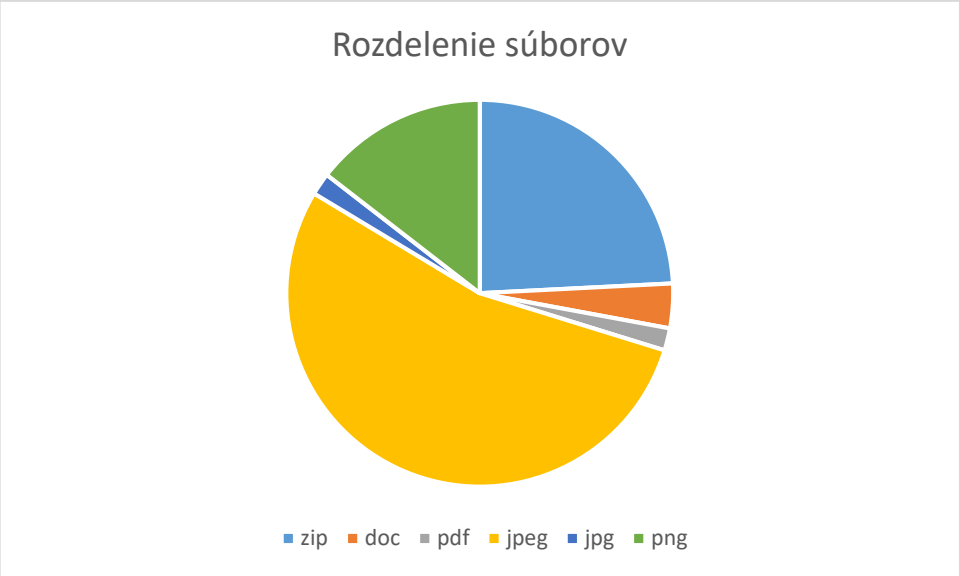
aby ich označili za nebezpečné. Adresy zo Spojeného kráľovstva mali počet hlásení menší, pričom len jedna z adries mala vyšší počet hlásení.

4.2 Súbory v emailoch

Niektoré z emailov obsahovali rôzne druhy súborov, pričom niektoré emaily obsahovali súborov aj viac. Súbory sú odosielané najčastejšie ako obrázky, aby bolo možné po otvorení takéhoto obrázku zobraziť nejakú reklamu, pomerne často sa však vyskytujú aj archívy ako je napr. archív s koncovkou .zip. Celkový počet súborov a ich rozdelenie je možné vidieť v tabuľke 2 a na obrázku 15:

Tabuľka 2 – Prehľad o celkovom počte súborov a o rozdelení súborov

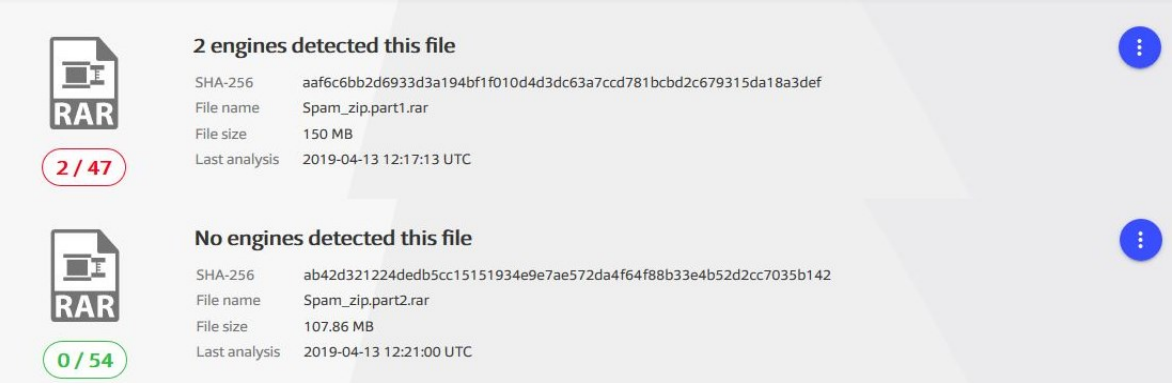
Počet súborov	**806**
Počet zip	195
Počet exe	0
Počet vsb	0
Počet jar	0
Počet doc	30
Počet docx	0
Počet pdf	15
Počet xml	0
Počet ixml	0
Počet jpeg	434
Počet jpg	15
Počet png	117



Obrázok 15 – Prehľad o rozdelení súborov z príloh

Celkový počet súborov v emailoch bol 806, čo tvorí približne 2% z celkového počtu emailov. Ako bolo predpokladané, obrázky sa ako prílohy vyskytovali najčastejšie, pričom 3 definované obrázkové typy dokopy tvorili 70% z celkového počtu súborov. Dokumenty, ktoré boli vo formáte .pdf a .doc sa celkovo vyskytli 45x, čo je 6% z celkového počtu. V balíku sa objavilo 195 .zip archívov, pričom tieto archívy predstavujú najväčšie bezpečnostné riziko. Práve v archívoch sa totiž môžu vírusy vyskytnúť najčastejšie, môžu v nich byť obsiahnuté nejaké spustiteľné súbory, ktoré by po spustení do počítača mohli nainštalovať škodlivý kód.

Súbory v emailoch boli podrobené antivírusovej kontrole. Balík poskytnutých emailov preverený internetovou službou VirusTotal. Táto stránka je celosvetovo uznávaná pre svoju antivírusovú kontrolu, pričom poskytnuté balíky a súbory posiela na kontrolu rôznym antivírusovým službám, ktoré súbory skontrolujú a v prípade, že by sa v balíku vírus nachádzal, ho označia za nebezpečný. Z dôvodu veľkosti balíku poskytnutých emailov bol tento balík rozdelený na 2 menšie balíky, pričom v týchto balíkoch len 2 zo 47 dostupných vyhľadávačov našli nejaký vírus, konkrétne sa jednalo o vyhľadávače ESET NOD32 a Zoner. ESET NOD32 hlásil vírus, ktorý niesol označenie Generik variácia, presnejší názov vírusu ESET zistiť nedokázal. Vyhľadávač Zoner zistil, že v balíku súborov sa nachádzajú vírusy nazývané trójsky kôň. Obidva vyhľadávače, ktoré sú celosvetovo známe teda označili balík týchto emailov za nebezpečný. Presný výstup zo stránky VirusTotal je viditeľný na obrázku 16:

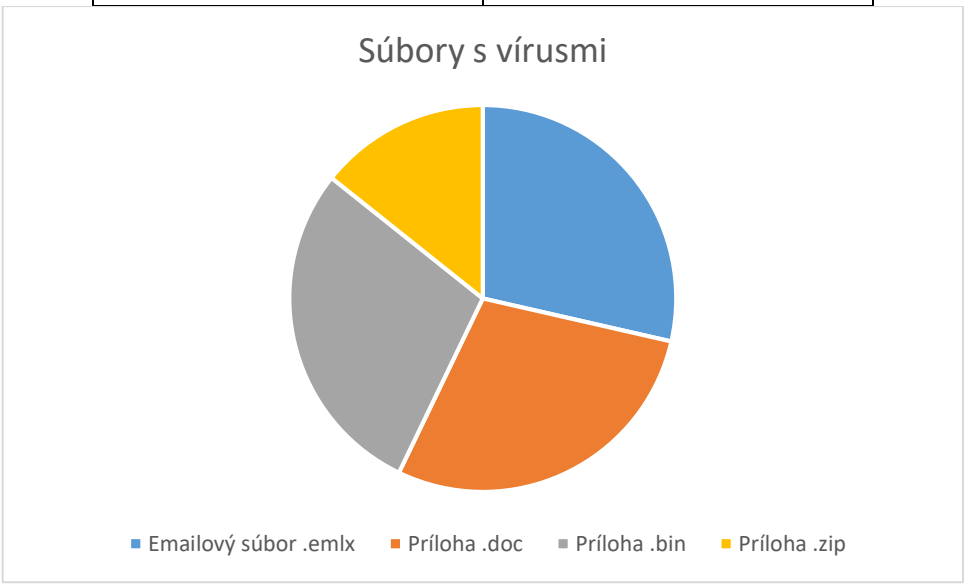


Obrázok 16 – Výstup zo stránky VirusTotal

Balíky boli následne rozbalené a skontrolované svetovo uznávaným antivírusovým programom Malwarebytes, ktorému sa však podarilo zistiť len jednu hrozbu. Zvyšný počet hrozieb bol automaticky zmazaný antivírusovou službou Windows Defender, ktorá aj cez deaktiváciu naďalej tieto súbory blokovala. Programy Malwarebytes a Windows Defender spoločne našli 7 vírusov. Konkrétny počet nájdených hrozieb pri rôznych koncovkých je možné vidieť v tabuľke 3 a grafickú reprezentáciu tohto rozdelenia na obrázku 17:

Tabuľka 3 – Vírusy v súboroch podľa koncoviek

Celkovo	**7**
Emailový súbor .emlx	2
Príloha .doc	2
Príloha .bin	2
Príloha .zip	1



Obrázok 17 – Rozdelenie súborov s vírusmi podľa koncoviek

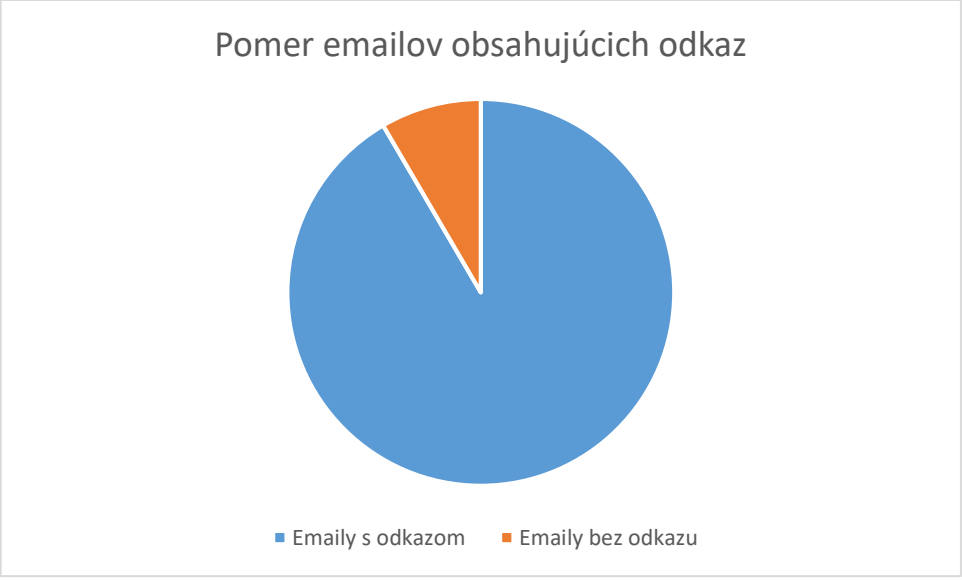
4.3 Emaily s odkazom

V emailoch môžu byť často zahrnuté rôzne odkazy, ktoré vedú na iné stránky. Môže sa jednať o stránky, na ktorých sú umiestnené nejaké reklamy alebo o stránku, na ktorej je možné sa odhlásiť z odoberania noviniek. Odhlásenie sa z odoberania noviniek by malo vykonať akciu, po ktorej by spamové emaily z danej adresy viac chodiť nemali. Môže sa však stať, že práve odkaz na zrušenie odberu môže byť odkaz vedúci na stránku so škodlivým kódom, popr. na stránku, kde užívateľ musí vyplniť svoje osobné údaje pre zrušenie odberu. Vyplnenie týchto osobných údajov by mohlo spôsobiť to, že tieto údaje budú použité aj bez súhlasu užívateľa, popr. budú zneužité.

Môže sa tiež stať, že odkaz, ktorý sa nachádza v obsahu emailu, môže viesť práve na podvodnú stránku banky, stránku nejakého úradu či organizácie a pod., ktorá bola vytvorená za účelom získania osobných údajov od užívateľa. S pomocou vytvorených skriptov boli skontrolované všetky poskytnuté emailové súbory, čím sa docielilo zistenie presného počtu súborov s odkazom a celkový počet odkazov. Výsledky je možné vidieť v tabuľke 4 a graficky reprezentované na obrázku 18:

Tabuľka 4 – Počet emailov s odkazom a celkový počet odkazov v súboroch

Emaily bez odkazu	3456
Emaily s odkazom	37573
Počet odkazov v emailoch celkovo	121480

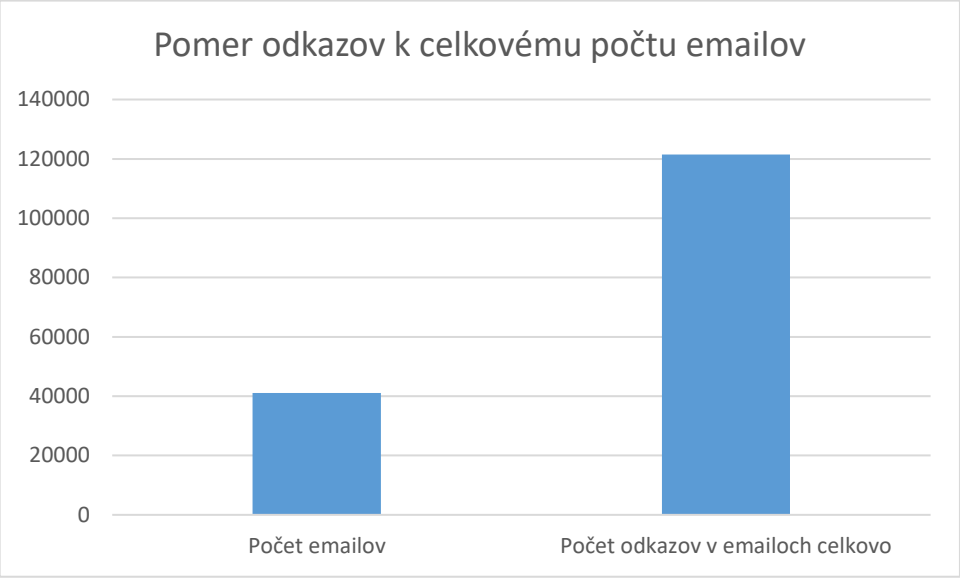


Obrázok 18 – Pomer emailov obsahujúcich odkaz

Z výsledkov je zrejmé, že takmer 92% zo všetkých emailov obsahovalo aspoň jeden odkaz. Nie je však možné analyzovať, či sa jedná o pharming alebo phishing. K takejto analýze by bolo potrebné použiť už existujúcu databázu kľúčových slov. S istotou sa však dá povedať, že v emailoch sa nejaký druh scamu nachádza. Aj keď väčšina emailov odkaz obsahovala, neznamená to, že sú tieto odkazy škodlivé alebo vedú na stránku s reklamou. Môže sa tiež stať, že email, ktorý odkazuje na obrázok dostupný práve z nejakého odkazu je započítaný do kategórie emailov s odkazom.

Vo väčšine prípadov by mohlo byť nebezpečné takéto otváranie odkazov, v reálnom svete je bezpečné otvárať len tie odkazy, u ktorých si je užívateľ istý, že sú bezpečné, napr. email obdržaný po registrácii na diskusné fórum alebo po objednávke tovaru z internetu.

Celkový počet odkazov v emailoch bol 121480, čo je niekoľkonásobne viac ako bol počet emailov celkovo. Každý email podľa štatistiky obsahuje priemerne 2,96 odkazu. Grafické porovnanie je zobrazené na obrázku 19:



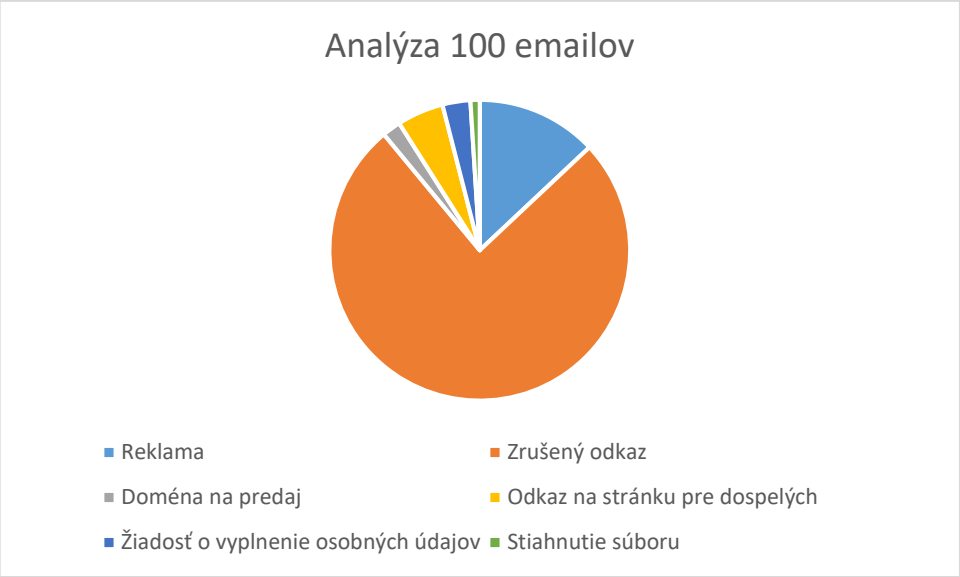
Obrázok 19 – Pomer odkazov k celkovému počtu emailov

Keďže nie je dostupná analýza a triedenie emailov do kategórií, ručne bolo analyzovaných 100 emailov, pri ktorých boli otvárané odkazy. Výsledky boli zhrnuté do 6 rôznych kategórií, ktoré je možné vidieť aj s počtom opakovaní v tabuľke 5:

Tabuľka 5 – Prehľad o kategóriách emailov s odkazom

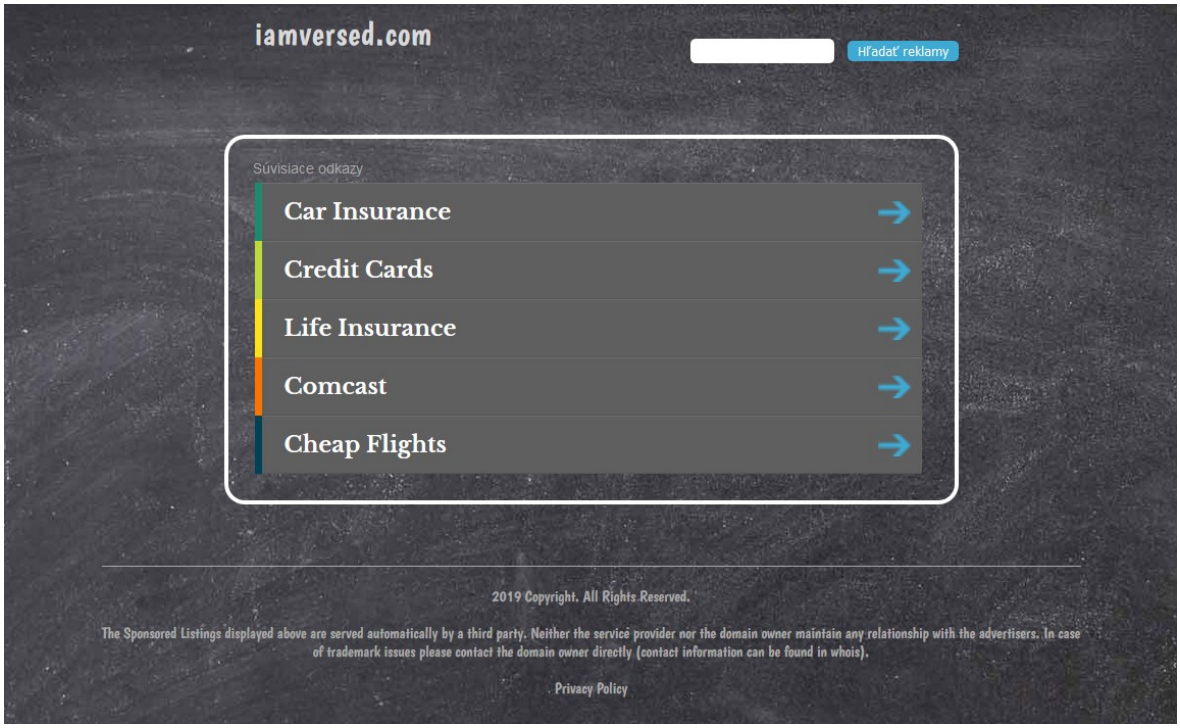
Reklama	13
Zrušený odkaz	76
Doména na predaj	2
Odkaz na stránku pre dospelých	5
Žiadosť o vyplnenie osobných údajov	3
Stiahnutie súboru	1

Grafický prehľad je možné vidieť na obrázku 20:



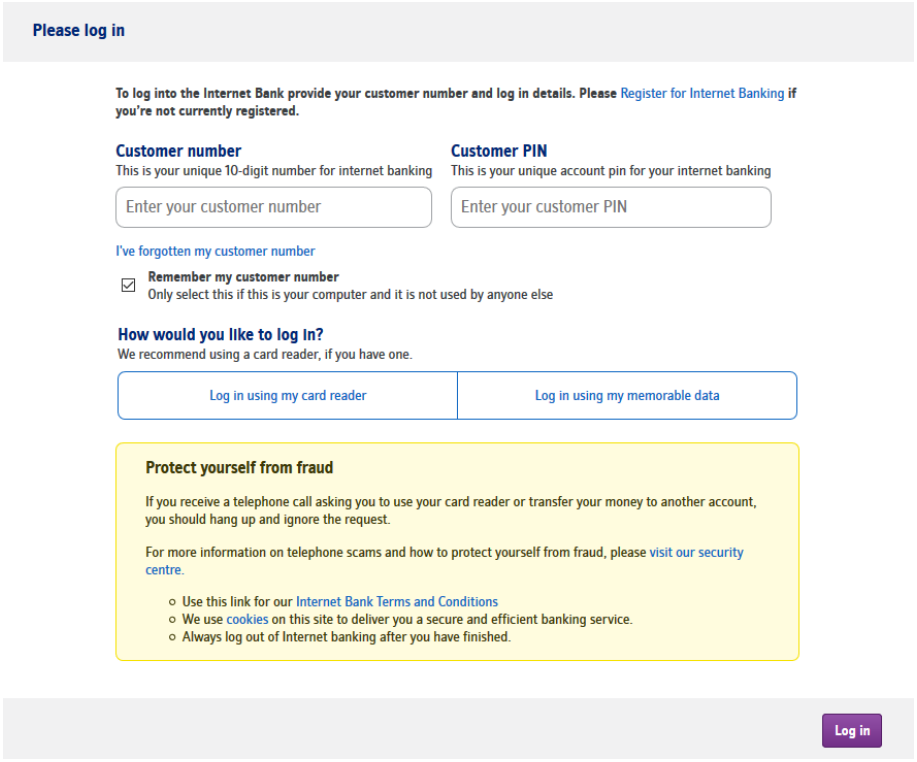
Obrázok 20 – Prehľad o kategorizácii emailov pri analyzovaní 100 emailov

Z obrázku 20 a tabuľky 5 jasne vyplýva fakt, že najväčšia časť týchto odkazov bola nefunkčná, teda je možné, že odkazy porušovali určité práva a nariadenia, popr. boli stránky nevhodné a nahlásené, čo viedlo k ich zrušeniu. Čím starší email bol, tým bola väčšia šanca na nefunkčný odkaz. Novšie emaily obsahovali reklamy častejšie, jeden email dokonca žiadal povolenie na stiahnutie súboru s príponou .exe. Stránka ponúkajúca reklamy je znázornená na obrázku 21:



Obrázok 21 – Stránka ponúkajúca reklamy a odkazy

Niektoré domény pravdepodobne prestali byť platené, čo viedlo k ponúknutiu tejto domény na predaj. Z celkového počtu 100 analyzovaných emailov obsahovalo odkaz na stránku s nevhodným obsahom, ktorý bol určený pre dospelé osoby 5 stránok, taktiež sa objavili tri odkazy vedúce na stránku banky či inštitúcie. Z týchto troch odkazov viedli dva na stránku, kde útočníci chceli osobné údaje ako meno, priezvisko, telefónne číslo, email a adresu. Zvyšný 1 odkaz viedol na stránku, ktorá vypadala ako banka, kde bolo vyžadované číslo bankového účtu a tiež bezpečnostný kód k účtu. Presný príklad takejto stránky je vidieť na obrázku 22:



Obrázok 22 – Podvodná stránka žiadajúca o vyplnenie osobných údajov

Stránka z obrázku 22 sa javí ako stránka banky NationWide, jedná sa pritom ale len o kópiu tejto stránky, ktorá je už nahlásená a internetový prehliadač umožní na stránku vstúpiť len po upozornení, že sa jedná o falošnú stránku. Stránka banky NationWide pritom bola napadnutá niekoľkokrát, pričom banka podnikla všetky potrebné kroky, aby sa nemohlo stať to, že užívateľ bude bez varovania na takúto stránku pripustený a stratí svoje osobné údaje. V prípade vyplnenia takýchto údajov by bolo totiž takmer isté, že užívateľ, ktorý tieto údaje vyplnil, by prišiel o finančný obnos.

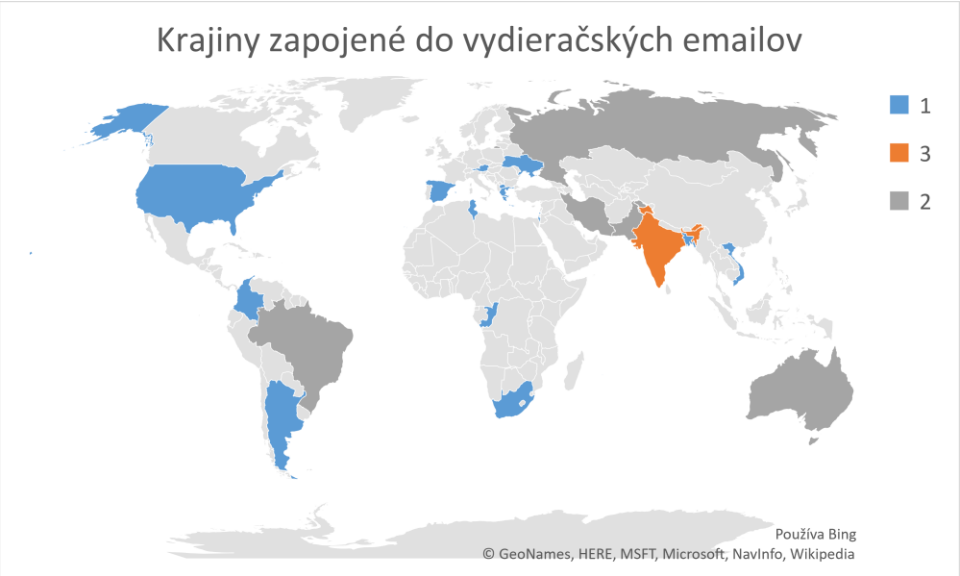
5 VYDIERAČSKÉ EMAILY

Samotnú kapitolu si zaslúžia vydieračské emaily, ktoré sú jedným z najväčších problémov súčasnosti v rámci spamových emailov. Tieto vydieračské emaily môžu byť v rôznych jazykoch, útočníci môžu byť z rôznych krajín a môžu používať iné metódy pre získanie finančného obnosu. Útočníci žiadajú sumu, ktorá býva zväčša uvedená v dolároch a dožadujú od svojej obete zaplatenie tohto obnosu peňazí vo virtuálnej mene bitcoin na poskytnutú peňaženku. Útočníci varujú, že ak obeť túto sumu na uvedenú peňaženku nepošle, budú zverejnené ich intímne fotografie alebo osobné údaje a pod.

Pomocou vytvorených skriptov boli analyzované všetky dostupné emailové súbory a boli v nich vyhľadávané tri kľúčové slovíčka, konkrétne slová **BTC**, **bitcoin** a **wallet** a taktiež boli kontrolované emaily odosielateľov. Výsledkom zo skriptov bolo 30 nájdených vydieračských emailov, ktoré boli poslané z rôznych krajín sveta a v rôznych svetových jazykoch.

5.1 Krajiny

Tak, ako sa do rozposielania spamových emailov zapojilo celkovo 105 krajín, bol dostatočne veľký počet krajín zapojený aj do rozposielania vydieračských emailov. Presnejšie sa do rozposielania takýchto emailov zapojilo 23 krajín, v niektorých prípadoch prišli z jednej krajiny aj viaceré takéto emaily. Podrobnú mapu sveta s krajinami, ktoré sa zapojili do tejto nekalej činnosti je možné vidieť na obrázku 23:



Obrázok 23 – Mapa sveta s krajinami zapojenými do vydieračských emailov

Aj keď je India najľudnatejším štátom sveta, veľa ľudí tam denne prístup k internetu samotnému nemá. To ale očividne neodradzuje útočníkov, pretože práve India patrí k najfrekventovanejšej krajine, čo sa týka posielania takýchto vydieračských emailov. Nasleduje ju napr. Rusko, Brazília alebo Austrália. Zaujímavé je, že aj keď Spojené štáty americké poslali najviac spamových emailov celkovo, len jeden email z nich mal vydieračský obsah. Pri krajine, ktorá je technologicky na špičke sveta, bolo toto očakávané číslo väčšie. Štáty ako Izrael a Irán boli taktiež zapojené. Celkom prekvapivým výsledkom je Rakúsko, ktoré celkovo odoslalo len 3 spamové emaily, pričom jeden z nich je práve vydieračský email.

5.2 Jazyk

Angličtina, ako najviac používaný a najrozšírenejší svetový jazyk, je najčastejším použitým jazykom u útočníkov, ktorí vydieračské emaily píšu. Predpokladá sa, že v balíku zo svetovej databázy by boli vydieračské emaily písané práve najčastejšie v anglickom jazyku, útočníci sa však prispôsobujú a takéto emaily píšu už aj v iných jazykoch, čím sa snažia vzbudiť v čitateľovi vyšší záujem a vyvolať väčší strach. Použité jazyky z emailov, ktoré boli v poskytnutom balíku, je možné vidieť na obrázku 24:

Obrázok 24 – Použité jazyky v rámci vydieračských emailov

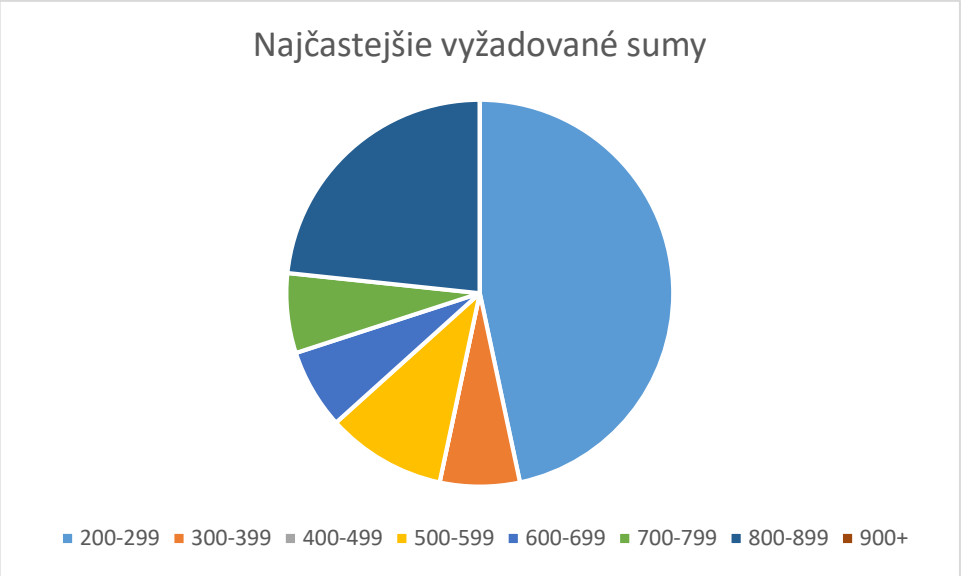
Z obrázku 24 jasne vyplýva, že angličtina ako najviac používaný svetový jazyk vedie nadpolovičnou väčšinou. Konkrétne z 30 vydieračských emailov bolo 17 napísaných v angličtine. Zaujímavým výsledkom je tiež to, že 11 z týchto emailov bolo napísaných

v češtine, aj keď sa zväčša jednalo o pochybnú češtinu preloženú pravdepodobne prekladačom od spoločnosti Google. Tieto emaily občas nedávali úplný zmysel, boli však prispôsobené aspoň trochu českému jazyku a tým môžu tieto vydieračské emaily vyvolávať horšie pocity hlavne u starších alebo menej znalých ľudí v Českej republike, ktorí porozumejú emailu tiež, čím sa zvyšuje šanca, že odošlú útočníkovi žiadanú sumu. Aj keď emaily chodili na české emailové schránky, našli sa medzi nimi aj 2 napísané v čínskom jazyku, z ktorých nebolo možné vyčítať nič iné než slovo bitcoin, sumu a samotnú bitcoinovú peňaženku.

Samotný text takýchto emailov sa často opakoval, bolo použitých len pár rôznych textov, pričom niektoré boli zastrašujúce len trochu, útočník v nich dokonca poprial svojej obeti veľa šťastia, popr. sa aj predstavil. Samotné texty sa opakovali či už v tom, ako útočník peniaze žiadal alebo v tom, čo sa stane ak obeť tieto peniaze nepošle. Taktiež všetci útočníci zdôrazňovali, aby si obeť skontrolovala z akého emailu toto vydieranie prišlo, aby tým vyvolali ešte väčší strach v užívateľovi, ktorý si všimne, že email bol poslaný z jeho vlastného účtu. Jeden z týchto emailov bol však nie len vydieračský, ale aj výhražný, kedy útočník dáva na výber presne dve možnosti, čo môže jeho obeť spraviť. Taktiež pripomína obeti aby sa ani nesnažila volať na políciu, pretože sa im aj tak útočníka vypátrať nepodarí a viedlo by to k zničeniu života obete.

5.3 Sumy

Tak, ako boli používané rôzne jazyky, tak útočníci žiadali aj rôzne sumy od svojich obetí. Po analýze týchto vydieračských emailov bolo vytvorených 8 kategórií s rôznymi rozmedziami súm, aby bolo lepšie vidieť, v akom rozmedzí útočníci financie žiadajú najviac. Niektoré rozmedzia neboli ani žiadané, to ale neznamená, že na inom balíku emailov by žiadané neboli. Rozmedzia týchto súm a počet žiadaní sumy z konkrétneho rozmedzia je možné vidieť na obrázku 25:



Obrázok 25 – Sumy ktoré útočníci žiadali

Z grafického znázornenia je možné vidieť, že najčastejšie, konkrétne 14x, boli žiadané sumy v rozmedzí 200 až 299 dolárov. Aj keď je táto suma malá, útočníci v nej vidia najväčší potenciál. Je to spôsobené asi tým, že táto suma nemusí prísť ľuďom veľmi vysoká a uhradia ju pravdepodobne skôr ako sumu dvojnásobne vyššiu. Nad 900 dolárov nežiadal ani jeden z útočníkov, naopak 23% útočníkov žiadalo sumu medzi 800 a 900 dolármi. Ostatné žiadané sumy boli práve medzi týmito sumami, pričom takmer vždy, až na jeden prípad boli uvedené v dolároch. Len v jednom z 30 emailov bola suma žiadaná v eurách, nie v dolároch. Ani jeden z útočníkov nežiadal sumu v korunách, aj keď cieľová emailová adresa bola česká.

5.4 Peňaženky

Pri vydieraní boli použité rôzne peňaženky. Niektorí útočníci používali rovnaké peňaženky, aj keď sa predstavili inak alebo napísali text v inom jazyku. Predpokladá sa, že tieto peňaženky fungujú len pre prijatie tohto obnosu peňazí, ktorý je následne preposlaný na iné peňaženky, čím sa zabráni jeho jednoduchému dopátraniu. Zoznam použitých peňaženiek a počet ich použití je možné vidieť na obrázku 26:

Obrázok 26 – Zoznam peňaženiek a ich použitie

Najväčší počet použití jednej peňaženky bol 3, pričom občas bola jedna peňaženka použitá aj na texty v rôznych jazykoch. Celkovo sa používalo 16 peňaženiek, pričom tieto neboli konečné. Aj keď na tieto peňaženky boli posielané sumy, ktoré vydierači žiadali, tie následne boli preposielané na peňaženky iné. Niekedy sa jednalo o pár transakcií priamo na iný účet, v niektorých prípadoch šlo o hromadne premyslenú metódu triedenia peňazí a o uistenie sa, že nikto tieto financie jednoducho nevystopuje. Počet transakcií a kam boli peniaze presmerované je možné vidieť v tabuľke 6:

Tabuľka 6 – Bitcoinové peňaženky a ich presmerovania

BTC peňaženka	Počet transakcií	Prijatých BTC	Presmerované	BTC na účte
1GL9JtXPRTPetx	55	1,739	1GEa2PsM5TnH	5
139XY4ZjWYqH	8	0,171	1GEa2PsM5TnH	5
1BSAHXc58m2D	12	0,547	1GEa2PsM5TnH	5
1MN7A7QqQaA	26	1,616	1GEa2PsM5TnH	5
1KGjDZ7RFV39r2	13	0,315	38nJGvXpyREpS7	57,124
17XHRucfd4kx3	15	1,328	1Kr6QSydW9bF	3668,53
1DVU5Q2HQ4sr	22	1,701	1FTa5nmDMetA	13,87
1B1Vov1LTLGLcV	18	1,943	1Kr6QSydW9bF	3668,53
19qL8vdRtk5xJc	19	1,423	1NDyJtNTjmwk5	13165,37
1JRCbCH9E3iLhS	10	0,442	18tsaq2YNfahCb	366,35
1P7bLeCJywaaD	11	0,854	bc1qc5srz2qn00	N/A
18QJdD5yWJyje	17	1,228	3NXPhnNYxjsE4Y	47,55
1Jh1miFmhTmG	50	6,503	1DVjDVADCHb3	N/A
145SmyE7DBEQ	78	10,431	12cUWYn6P23jC	36,054
142e8SgyTLnkvw	12	1,515	12cUWYn6P23jC	36,054
1GF8J1XRaiX2oH	13	2,277	1NDyJtNTjmwk5	13165,37

Prvé štyri peňaženky mali rôzny počet transakcií a tiež rôzny počet prijatých bitcoinov. To znamená, že rozličné metódy vydierania a rozličné obete spôsobili to, že aj keď na jednu peňaženku prišlo úplne minimum financií, na druhú naopak prišlo peňazí dosť. Tieto štyri peňaženky následne previedli svoj obnos na jeden finálny účet, ktorý má na svojom konte rovných 5 bitcoinov k dnešnému dátumu.

U niektorých peňaženiek boli tieto získané peniaze preposlané len niekoľkokrát a následne išli na finálnu peňaženku. U ostatných peňaženiek šlo o hromadné delenie na rôzne peňaženky. U jednej z peňaženiek nebolo možné zistiť kam peniaze išli, pretože bola buď zrušená, alebo skrytá. Jedna peňaženka taktiež rozoslala svoju hotovosť 6,503 BTC na niekoľko desiatok ďalších peňaženiek súčasne, preto nebolo možné zistiť, kde peniaze skončili.

Najzaujímavejším zistením ale bolo, že niektoré z peňaženiek preposielali získanú sumu niekoľko desiatok krát na rôzne účty, ktoré boli použité len jednorazovo a skončili na účtoch, kde momentálny počet BTC presahuje pár tisíc. U peňaženky 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s to bolo dokonca tak rozsiahle, že cez túto peňaženku dokopy prešlo cez 5 miliónov bitcoinov a počet transakcií z alebo na túto peňaženku bol viac ako 400 tisíc. Aktuálny počet bitcoinov na tejto adrese bol 13165 BTC,

čo je v prepočte na doláre približne 66 miliónov amerických dolárov. Aj keď celá táto suma pravdepodobne nie je zložená len z vydieračských emailov, financie z nich tam putujú taktiež.

5.5 Kontrola IP

Adresy, ktoré posielali vydieračské emaily, majú najväčšiu šancu nahlásenia za obťažovanie, popr. práve za vydieranie. Keďže spolu so zoznamom, odkiaľ tieto vydieračské emaily chodili je k dispozícii aj zoznam IP adries, boli tieto IP adresy preverené rôznymi internetovými službami, ktoré zistia, či už táto vydieračská adresa nahlásená niekým bola, alebo nie. Na zistenie počtu nahlásení bola opäť použitá stránka AbuseIPDB.com, z ktorej výsledky je možné vidieť na obrázku 27:

Obrázok 27 – Počet hlásení u vydieračských adries

Niektoré adresy z krajín sveta neboli nahlásené vôbec, naopak najviac bola nahlasovaná adresa, ktorá pochádzala z Tuniska. Táto adresa mala tak veľký počet hlásení, že ak by boli spočítané hlásenia u všetkých ostatných adries, nedosiahli by v súčte ani polovicu z hlásení na IP adresu z Tuniska. Stránka však tieto adresy kontroluje dôkladnejšie a poskytuje približný prehľad o tom, aká je pravdepodobnosť, že je stránka škodlivá, popr. obsahuje malware a pod. Adresa z Tuniska mala túto pravdepodobnosť 28%, čo je najviac zo všetkých kontrolovaných IP adries, ktoré sa do týchto výhražných emailov v rámci tohto balíku zapojili. Adresa z Dominikánskej republiky má túto pravdepodobnosť 14%, čím sa radí na

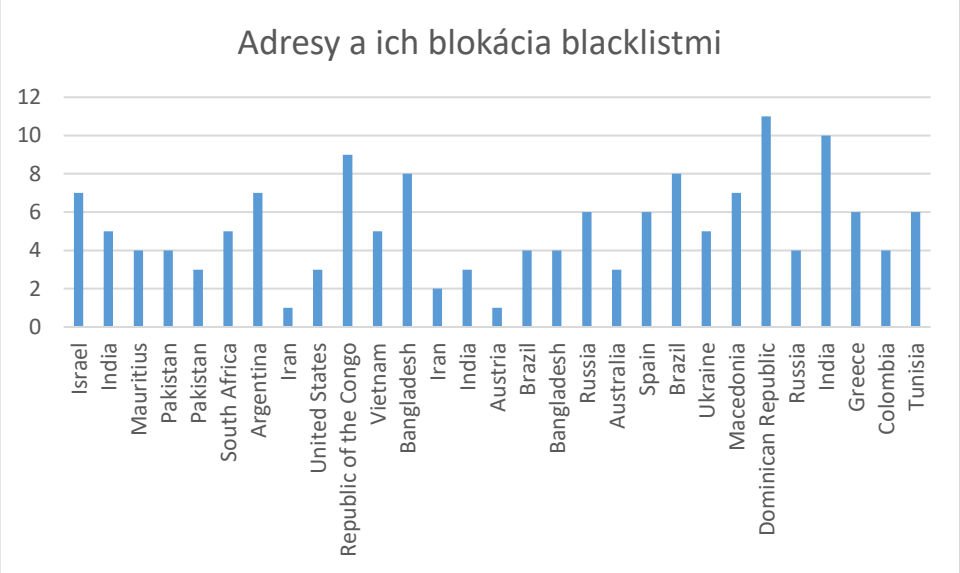
druhé miesto. U ostatných adries bola táto pravdepodobnosť 0%, čo podľa stránky značí, že tieto adresy nie sú nijak škodlivé.

Keďže počet nahlásení u týchto adries bol malý, bola vykonaná ďalšia kontrola týchto adries pomocou inej stránky, kde je možné si overiť to, na koľkých blacklistoch sa tieto adresy nachádzajú. K tomu bola použitá stránka whatismyipaddress.com, ktorá má zoznam 80 antispamových databáz, u ktorých sú tieto adresy preverované. Zoznam adries aj s počtom blacklistov, na ktorých boli zablokované, je možné vidieť v tabuľke 7:

Tabuľka 7 – Zoznam adries a počet blokácií blacklistmi

Krajina	IP adresa	Počet blacklistov
Izrael	79.177.233.5	7
India	45.117.181.150	5
Maurícius	197.226.193.10	4
Pakistan	39.48.54.25	4
Pakistan	39.46.195.193	3
Južná Afrika	41.13.88.235	5
Argentína	181.225.202.44	7
Irán	188.212.87.13	1
Spojené štáty americké	206.251.60.213	3
Kongo	169.255.121.237	9
Vietnam	113.182.182.233	5
Bangladéš	103.89.244.206	8
Irán	31.14.95.214	2
India	27.57.33.121	3
Rakúsko	192.164.153.120	1
Brazília	191.181.67.126	4
Bangladéš	103.110.217.20	4
Rusko	194.28.215.91	6
Austrália	203.63.42.145	3
Španielsko	37.134.150.0	6
Brazília	45.5.199.250	8
Ukrajina	93.74.42.53	5
Macedónsko	77.29.95.207	7
Dominikánska republika	186.120.31.212	11
Rusko	80.89.157.8	4
India	114.29.236.151	10
Grécko	89.210.175.95	6
Kolumbia	191.109.179.106	4
Tunisko	213.150.170.158	6

Tunisko, ktoré bolo nahlásené najviac v rámci vydieračských adries, sa na blackliste databáz nevyskytuje úplne najčastejšie. Najčastejšie sa vyskytuje IP adresa z Dominikánskej republiky, druhá v poradí je India, nasledovaná Kongom. Na rozdiel od počtu hlásení, kde niektoré IP adresy prešli bez jediného nahlásenia, sa v databáze blacklistov každá z týchto adries vyskytuje aspoň raz. Najmenej sa na zozname blacklistov vyskytovala adresa z Iránu, ktorá bola zablokovaná len jednou antispamovou službou. Grafické znázornenie tejto tabuľky je znázornené na obrázku 28:



Obrázok 28 – Adresy a ich blokácia blacklistmi

6 ZHRNUTIE

Táto kapitola je venovaná zhrnutiu všetkých zistených údajov z poskytnutých spamových emailov. Bude obsahovať hlavne tabuľky, v ktorých budú zaznamenané najdôležitejšie zistenia z celej práce. Prehľad zistených informácií z práce je možné vidieť v tabuľke 8:

Tabuľka 8 – Prehľad o zistenej štatistike

Celkový počet emailov	41072
Počet spracovaných emailov	41029
Počet zapojených krajín	105
Najaktívnejšie krajina	Spojené štáty americké
Najaktívnejší spamer	Holandsko
Počet emailov so súborom	806
Počet súborov s vírusom	7
Počet emailov s odkazom	37573
Počet odkazov celkovo	121480
Počet vydieračských emailov	30
Krajín zapojených do blackmailingu	23
Počet bitcoinových peňaženiek	16

Z tabuľky 8 jasne vyplýva, že najaktívnejšia krajina sú Spojené štáty americké, čo je vysvetliteľné hlavne tým, že sa jedná o jednu z najviac rozvinutých krajín na svete. V tejto časti sveta má obrovský počet obyvateľov prístup k internetu a taktiež je tam veľké množstvo spoločností a organizácií ktoré môžu takéto emaily rozposielať. Aj keď najviac emailov prišlo práve z USA, najaktívnejší spameri boli z Holandska, odkiaľ najaktívnejší spamer odoslal 123 emailov. Bližší prehľad o zapojených a o najaktívnejších krajinách je v kapitole 4.1.

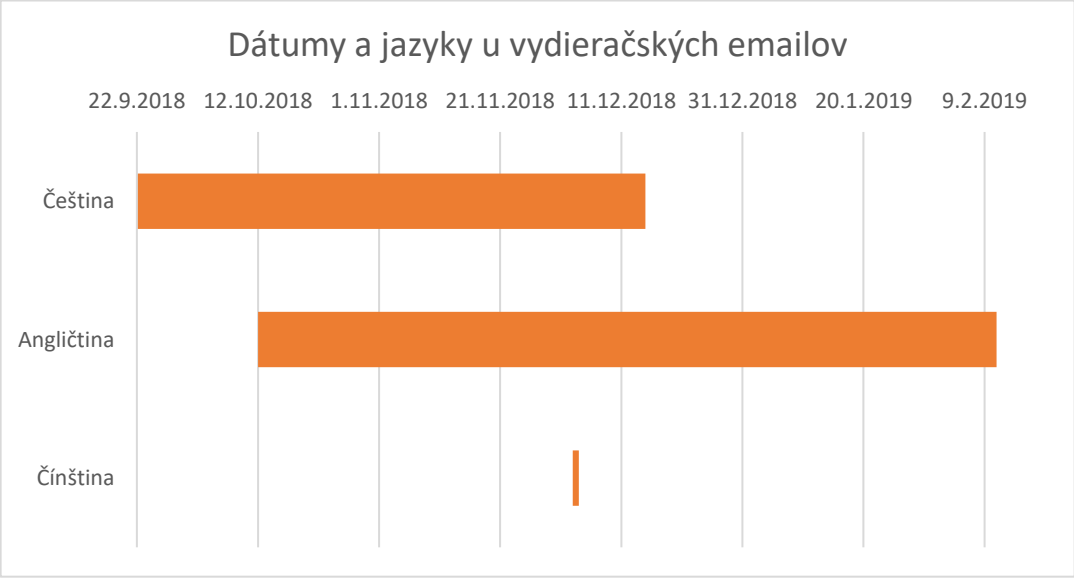
Vytvorené skripty nevedia rozpoznať, či sa jedná o email ktorý by bol zaradený do kategórie phishing, pharming alebo či sa jedná o reklamu. Z tohto dôvodu bola vykonaná ručná analýza 100 emailových súborov, z ktorých boli otvárané odkazy pre približný prehľad o zaradení do týchto kategórií. Z analýza vyplynulo, že 13% emailov s odkazom tvorilo odkaz práve na stránku s reklamou, naopak 5% tvorilo odkaz na stránku s nevhodným obsahom. Medzi phishing by sa mohli zaradiť 3% z emailov s odkazom, kde odkazy otvorili falošnú stránku banky alebo inštitúcie, ktorá žiadala vyplnenie osobných údajov, v horšom prípade prihlasovacie údaje, čo by takmer iste viedlo k strate osobných údajov. Za pharming by sa dalo označiť 1% emailov, kde stránka z odkazu pri prehliadaní presmeruje užívateľa

na falošnú stránku alebo na stránku kde chcelo byť zahájené sťahovanie súboru so škodlivým kódom. Vzhľadom k tomu že sú emaily staršieho dátumu, 76% zo stránok už bolo zrušených alebo zablokovaných. Presnejší prehľad o emailoch s odkazom je v kapitole 4.3, kde sú zobrazené aj ukážky takýchto emailov. Tento približný prehľad a percentá sa však môžu meniť v závislosti na použitom balíku alebo pri otváraní iných emailových správ, prehľad je skutočne len orientačný.

Práca bola z veľkej časti venovaná aj vydieračským emailov (blackmailingu), ktorý je veľkým problémom súčasnosti. Z takýchto vydieračských emailov boli zistené použité jazyky a podrobnejšie informácie o ich používaní, teda kedy sa používať začali a kedy skončili. Z nich bol následne vytvorený Ganttov diagram, na ktorom je možné lepšie vidieť jednotlivé časové úseky používania jazykov. Dátumy sú zobrazené v tabuľke 9 a na obrázku 29:

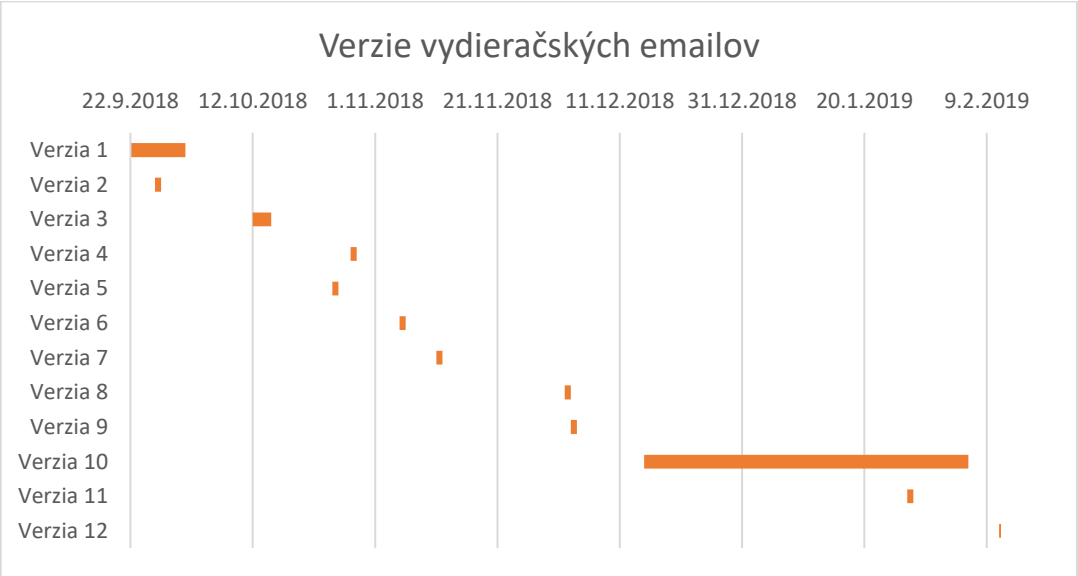
Tabuľka 9 – Dátumy a jazyky u vydieračských emailov

Jazyk	Štart	Koniec	Trvanie v dňoch
Čeština	22.9.2018	15.12.2018	84
Angličtina	12.10.2018	11.2.2019	122
Čínština	3.12.2018	3.12.2018	1



Obrázok 29 – Dátumy a jazyky u vydieračských emailov

Okrem rôznych použitých jazykov boli použité aj rôzne verzie textov, ktorými sa útočníci snažili svoju obeť zneistiť a získať tak od nej finančnú hotovosť v mene bitcoin. Niektoré z verzií boli používané dlhšie obdobie, pričom bola rovnaká verzia použitá aj v anglickom aj v českom jazyku, pričom v českom jazyku šlo najpravdepodobnejšie o preklad cez službu Google Translator. Niektoré z verzií boli naopak použité jednorazovo, popr. boli použité niekoľkokrát, ale všetky takéto emaily prišli na adresy v priebehu jedného dňa. Presnejší pohľad na Ganttov diagram so zobrazenými časovými úsekmi je zobrazený na obrázku 30:



Obrázok 30 – Verzie vydieračských emailov

ZÁVER

Cieľom práce bolo popísať terminológiu v rámci spamových emailov a priblížiť čitateľom hrozbu, ktorú tieto spamové emaily predstavujú. Tomuto faktu sa podľa môjho názoru nevenuje dostatočná pozornosť, pričom práve kvôli spamovým emailom dochádza na celom svete k miliónovým stratám. V teoretickej časti práce som definoval a následne popísal základné druhy spamových emailov, ktoré často končia v emailových schránkach. Sú nimi napr. hoax, ktoré vnímam ako problém súčasnosti, keďže dochádza k zosmiešňovaniu užívateľov a k poplašným správam, ktoré vyvolávajú paniku a sú šírené cez sociálne siete a emaily. K ukradnutiu identity a citlivých osobných údajov dochádza prostredníctvom spamových emailov, ktoré patria do kategórii pharming a phishing. Tieto fungujú najmä vďaka prílišnej dôverčivosti užívateľov, ktorí často poskytnú svoje osobné údaje alebo financie bez overenia, či stránka, na ktorú sa prihlasujú je skutočne dôveryhodná. Taktiež môže dôjsť k finančným stratám s víziou rýchleho obohatenia sa v prípadoch emailov, ktoré patria do kategórie Nigerian 419.

Po popísaní rozdielov som navrhol a vytvoril skripty, ktorých cieľom bolo zanalyzovať a následne vytriediť spamové emaily, zahrňujúce všetky vyššie uvedené kategórie. Výstupom zo skriptov je súbor, obsahujúci zistené IP adresy odosielateľov, počet emailov z týchto adries, krajiny odkiaľ odosielatelia pochádzajú, počet súborov a odkazov v emailoch. Pomocou skriptov je tiež možné zistiť, či sa jedná o email s vydieračských charakterom.

Po kompletnej analýze balíku emailov som sa utvrdil v tom, že hlavným problémom sú vydieračské emaily, ktoré sa čoraz viac rozširujú a útočníci žiadajú od svojich obetí výkupné v rôznych menách a sumách. V neposlednom rade môže ale dôjsť aj k poškodeniu systému počítača otvorením súboru obsahujúceho škodlivý kód, ktorý sa môže v prílohe emailu vyskytovať. Ďalej môže dôjsť k rizikám spojených s otvorením odkazu, vedúceho na falošnú internetovú stránku, a tým môže dôjsť k strate osobných údajov užívateľa. Aj keď zo svetových štatistík vyplýva, že najviac spamových emailov pochádza práve z Číny, z mnou analyzovanej vzorky bolo zistené, že Čína sa z celkového počtu krajín, ktoré boli do odosielania takýchto emailov zapojené, neumiestnila ani v rebríčku 10 najväčších odosielateľov. Ďalším zistením, ktoré bolo však z veľkej časti očakávané je fakt, že najväčším odosielateľom spamových emailov sú Spojené štáty americké. Čo sa samotných

odosielateľov, respektíve spamerov týka, tí najaktívnejší pochádzajú z Holandska. Samostatné zhrnutie je možné vidieť v kapitole 6, ktorá sa zhrnutiu venuje.

Prínosom tejto práce je hlavne to, že bežný neskúsený užívateľ si môže vytvoriť vlastnú mienku o tom, v akých počtoch sa emaily odosielajú, a môže bližšie pochopiť problematiku spamových emailov. Práca viedla práve k objasneniu terminológie, ktorá bola popísaná v teoretickej časti, a tiež ku kategorizácii veľkého množstva spamových emailov, k čomu boli použité práve vytvorené skripty. Do budúcna je prácu možné využiť ako učebnú pomôcku pre pochopenie spamu, vydieračských emailov a ostatných kategórií, ale tiež môže byť použitá ako štatistika o spamových emailoch, ktoré prichádzajú na českú emailovú adresu. Taktiež môžu byť využité skripty, ktoré boli pre prácu vytvorené, čím bude možné kategorizovať akýkoľvek poskytnutý balík, ktorý bude spĺňať kritériá.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Aktuálne hrozby a riziká v e-mailovej komunikácii. *Zoznam.sk* [online]. [cit. 2019-05-01]. Dostupné z: https://mail.zoznam.sk/help/protispamu

[2] Origin of the term „spam“ to mean net abuse. *Templetons.com* [online]. [cit. 2019-04-23]. Dostupné z: https://www.templetons.com/brad/spamterm.html

[3] Spam. *Britannica.com* [online]. [cit. 2019-04-23]. Dostupné z: https://www.britannica.com/topic/spam#ref1072166

[4] Spam statistics: spam e-mail traffic share 2018. *Statista.com* [online]. [cit. 2019-04-23]. Dostupné z: https://www.statista.com/statistics/420391/spam-email-traffic-share/

[5] MCDONALD, Alistair. *SpamAssassin: A Practical Guide to Integration and Configuration* [online]. Packt Publishing, 2004 [cit. 2019-04-23]. ISBN 978-1904811121.

[6] Ham v Spam: what’s the difference?. *Blog.barracuda.com* [online]. [cit. 2019-04-23]. Dostupné z: https://blog.barracuda.com/2013/10/03/ham-v-spam-whats-the-difference/

[7] MACDOUGALL, Curtis. *Hoaxes*. 2nd edition. Dover Pubns, 1958. ISBN 978-0486204659.

[8] Co je to hoax. *Hoax.cz* [online]. [cit. 2019-04-23]. Dostupné z: http://hoax.cz/hoax/co-je-to-hoax

[9] Scam. *Businessdictionary.com* [online]. [cit. 2019-04-23]. Dostupné z: http://www.businessdictionary.com/definition/scam.html

[10] I got a phishing email that tried to blackmail me – what should I do?. *Theguardian.com* [online]. [cit. 2019-05-05]. Dostupné z: https://www.theguardian.com/technology/askjack/2019/jan/17/phishing-email-blackmail-sextortion-webcam

[11] How to differentiate between spam and phishing emails?. *Quickheal.com* [online]. [cit. 2019-04-23]. Dostupné z: https://blogs.quickheal.com/differentiate-spam-phishing-emails/

[12] What is Spear Phishing?. *Kaspersky.com* [online]. [cit. 2019-04-23]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/spear-phishing

[13] What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. *Digitalguardian.com* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

[14] Phishing a Pharming. *Bezpecnyinternet.cz* [online]. [cit. 2019-05-01]. Dostupné z: http://m.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[15] DONOVAN, Felicia a Kristyn BERNIER. *Cyber Crime Fighters: Tales from the Trenches* [online]. Que Publishing, 2008 [cit. 2019-04-23]. ISBN 978-0789739223.

[16] Nigerian scams. *Scamwatch.gov.au* [online]. [cit. 2019-04-23]. Dostupné z: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

[17] ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* [online]. O'Reilly Media, 2014 [cit. 2019-04-23]. ISBN 978-1449374044.

[18] PATTERSON, Sam. *Bitcoin Beginner: A Step By Step Guide To Buying, Selling And Investing In Bitcoins* [online]. 2017 [cit. 2019-04-23].

[19] A Short History Of Bitcoin And Crypto Currency Everyone Should Read. *Forbes.com* [online]. 2017 [cit. 2019-04-23]. Dostupné z: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#7ebb168c3f27

[20] FORRESTER, Daniel a Mark SOLOMON. *Bitcoin Explained: Today's Complete Guide to Tomorrow's Currency* [online]. CreateSpace Independent Publishing Platform, 2013 [cit. 2019-04-23]. ISBN 978-1494296421.

[21] Phishing. *Scamwatch.gov.au* [online]. [cit. 2019-04-23]. Dostupné z: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing

[22] Spam and phishing in 2018. *Securelist.com* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://securelist.com/spam-and-phishing-in-2018/89701/

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

IP	Internet Protocol
DEC	Digital Equipment Corporation
BTC	Bitcoin
RegEx	Regular Expression (regulárny výraz)
API	Application programming interface (rozhranie pre programovanie aplikácii)
JSON	JavaScript Object Notation (JavaSkriptový objektový zápis)

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: OBSAH CD

Štruktúra obsahu priloženého na CD:

- **Text bakalárskej práce** – obsahuje text bakalárskej práce vo formáte PDF
- **Bakalárska práca výstup** – obsahuje všetky dáta zistené z archívu spamových emailov, taktiež sú obsiahnuté štatistiky a grafy
- Adresár **Zdrojové kódy –** obsahuje všetky zdrojové kódy s príponou .py programovacieho jazyka Python verzie 3.x potrebnej k spustení navrhnutej aplikácie pre kategorizáciu spamových emailov
- Adresár **Vydieračské emaily** – obsahuje všetky vydieračské emaily s príponou .emlx
- Archív **Spam, ham, phishing, viry, apod. –** obsahuje všetky dostupné spamové emaily aj s ich prílohami, heslo k archívu je BP2019

PRÍLOHA P II: NÁHĽAD VERZIÍ VYDIERAČSKÝCH EMAILOV

Verzia 1:

Ahoj, drahý uživatel utb.cz.
Do vašeho přístroje jsme nainstalovali jeden software RAT.
Pro tento okamžik je váš emailový účet napaden (viz , nyní mám přístup k vašim účtům)..
Stahoval jsem všechny důvěrné informace z vašeho systému a dostal jsem další důkazy.
Nejzajímavějším okamžikem, který jsem objevil, jsou videozáznamy o vás masturbující.
Zveřejnil jsem virus na pornografickém webu, a pak jste jej nainstalovali do svého operačního systému.
Po klepnutí na tlačítko Přehrát na porno video, v tom okamžiku byl můj trojan stažen do vašeho zařízení.
Po instalaci vám přední fotoaparát natáčí video pokaždé, když masturbujete, software se synchronizuje s vybraným videem.
Prozatím software získal všechny vaše kontaktní informace ze sociálních sítí a e-mailových adres.
Pokud potřebujete smazat všechny shromážděné údaje, pošlete mi $250 v BTC (krypto měně).
Toto je moje Bitcoin peněženka: 1GL9JtXPRTPetxgiJ8UcgrEECp12spD4tt
Máte 48 hodin po přečtení tohoto dopisu.
Po transakci vymažu všechna data.
Jinak posílám video se vaším žertíky všem vašim kolegům a přátelům!!
V budoucnosti buďte opatrnější
Navštivte prosím pouze zabezpečené weby!
Sbohem!

Verzia 2:

Ahoj!
Jsem členem mezinárodní hackerské skupiny.
Jak jste asi pravděpodobně uhodli, váš účet z domény@domain.com byl napaden, protože Poslal jsem vám e-mail z vašeho účtu.
V období od 5. července 2018 do 21. září 2018 jste byli infikováni virem, který jste vytvořili, prostřednictvím navštívených webových stránek pro dospělé.
Zatím máme přístup k vašim vzkazům, účtům sociálních médií a poslům.
Máme však úplné skládky těchto dat.
Jsme si vědomi svých malých a velkých tajemství ... jo, máte je.
Zaznamenali jsme a zaznamenávali vaše akce na pornografických webových stránkách. Váš vkus je tak divný, víte ..
Ale klíčovou věcí je, že jsme někdy zaznamenali vás s vaší webovou kamerou a synchronizovali nahrávky s tím, co jste sledovali!
Myslím, že nemáte zájem ukázat toto video svým přátelům, příbuzným a vašemu intimnímu ...
Přeneste 250$ do naší Bitcoin peněženky: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ
Garantuji, že po tom budeme smazat všechny vaše "data": D
Po přečtení této zprávy se spustí časovač. Máte 48 hodin na zaplacení výše uvedené částky.
Vaše údaje budou vymazány po převodu peněz.
V opačném případě budou všechny vaše záznamy a videozáznamy automaticky zaslány všem vašim kontaktům, které jsou na vašem zařízení nalezeny v okamžiku infekce.
Měli byste vždy myslet na vaši bezpečnost. Doufáme, že vás tento případ naučí udržovat tajemství.
Opatruj se.

Verzia 3:

Hello zacek@
My nickname in darknet is noll28.
I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.
Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.
I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.
I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!
I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created.
Send the above amount on my bitcoin wallet: 1MN7A7QqQaAVoxV4zdjdrnEHXmjhzcQ4Bq
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.
Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!
Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.
I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Verzia 4:

Hello!
I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.
Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.
Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account.
Through your e-mail, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a rat software on your device and long tome spying for you.
You are not my only victim, I usually lock devices and ask for a ransom.
But I was struck by the sites of intimate content that you very often visit.
I am in shock of your reach fantasies! Wow! I've never seen anything like this!
I did not even know that SUCH content could be so exciting!
So, when you had fun on intime sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I jointed them to the content of the currently viewed site.
Will be funny when I send these photos to your contacts! And if your relatives see it?
BUT I'm sure you don't want it. I definitely would not want to ...
I will not do this if you pay me a little amount.
I think $843 is a nice price for it!
I accept only Bitcoins.
My BTC wallet: 17XHRucfd4kx3W5ty7ySLGiKHqmPUUdpus
If you have difficulty with this - Ask Google "how to make a payment on a bitcoin wallet". It's easy.
After receiving the above amount, all your data will be immediately removed automatically.
My virus will also will be destroy itself from your operating system.
My Trojan have auto alert, after this email is looked, I will be know it!
You have 2 days (48 hours) for make a payment.
If this does not happen - all your contacts will get crazy shots with your dirty life!
And so that you do not obstruct me, your device will be locked (also after 48 hours)
Do not take this frivolously! This is the last warning!
Various security services or antiviruses won't help you for sure (I have already collected all your data).
Here are the recommendations of a professional:
Antiviruses do not help against modern malicious code. Just do not enter your passwords on unsafe sites!
I hope you will be prudent.
Bye.

Verzia 5:

Hello!
I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.
Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.
You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.
I am in shock of your fantasies! I've never seen anything like this!
So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.
There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.
Therefore, I expect payment from you for my silence.
I think $805 is an acceptable price for it!
Pay with Bitcoin.
My BTC wallet: 1DVU5Q2HQ4srFNSSaWBrVNMtL4pvBkfP5w
If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.
My Trojan have auto alert, after this email is read, I will be know it!
I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)
Do not be silly!
Police or friends won't help you for sure ...
p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.
I hope for your prudence.
Farewell.

Verzia 6:

I greet you!
I have bad news for you.
11/08/2018 - on this day I hacked your operating system and got full access to your account zacek@utb.cz
It is useless to change the password, my malware intercepts it every time.
How it was:
In the software of the router to which you were connected that day, there was a vulnerability.
I first hacked this router and placed my malicious code on it.
When you entered in the Internet, my trojan was installed on the operating system of your device.
After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).
A month ago, I wanted to lock your device and ask for a small amount of money to unlock.
But I looked at the sites that you regularly visit, and came to the big delight of your favorite resources.
I'm talking about sites for adults.
I want to say - you are a big pervert. You have unbridled fantasy!
After that, an idea came to my mind.
I made a screenshot of the intimate website where you have fun (you know what it is about, right?).
After that, I took off your joys (using the camera of your device). It turned out beautifully, do not hesitate.
I am strongly belive that you would not like to show these pictures to your relatives, friends or colleagues.
I think $849 is a very small amount for my silence.
Besides, I spent a lot of time on you!
I accept money only in Bitcoins.
My BTC wallet: 1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ
You do not know how to replenish a Bitcoin wallet?
In any search engine write "how to send money to btc wallet".
It's easier than send money to a credit card!
For payment you have a little more than two days (exactly 50 hours).
Do not worry, the timer will start at the moment when you open this letter. Yes, yes .. it has already started!
After payment, my virus and dirty photos with you self-destruct automatically.

Narrative, if I do not receive the specified amount from you, then your device will be blocked, and all your contacts will receive a photos with your "joys".
I want you to be prudent.
- Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)
- Do not try to contact me (this is not feasible, I sent you an email from your account)
- Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is already on a remote server.
P.S. I guarantee you that I will not disturb you again after payment, as you are not my single victim.
This is a hacker code of honor.
From now on, I advise you to use good antiviruses and update them regularly (several times a day)!
Don't be mad at me, everyone has their own work.
Farewell.

Verzia 7:

Dear user of fai.utb.cz!
I am a spyware software developer.
Your account has been hacked by me in the summer of 2018.
I understand that it is hard to believe, but here is my evidence (I sent you this email from your account).
The hacking was carried out using a hardware vulnerability through which you went online (Cisco router, vulnerability CVE-2018-0296).
I went around the security system in the router, installed an exploit there.
When you went online, my exploit downloaded my malicious code (rootkit) to your device.
This is driver software, I constantly updated it, so your antivirus is silent all time.
Since then I have been following you (I can connect to your device via the VNC protocol).
That is, I can see absolutely everything that you do, view and download your files and any data to yourself.
I also have access to the camera on your device, and I periodically take photos and videos with you.
At the moment, I have harvested a solid dirt... on you...
I saved all your email and chats from your messangers. I also saved the entire history of the sites you visit.
I note that it is useless to change the passwords. My malware update passwords from your accounts every times.
I know what you like hard funs (adult sites).
Oh, yes .. I'm know your secret life, which you are hiding from everyone.
Oh my God, what are your like... I saw THIS ... Oh, you dirty naughty person ... :)
I took photos and videos of your most passionate funs with adult content, and synchronized them in real time with the image of your camera.
Believe it turned out very high quality!
So, to the business!
I'm sure you don't want to show these files and visiting history to all your contacts.
Transfer $851 to my Bitcoin cryptocurrency wallet: 19qL8vdRtk5xJcGNVk3WruuSyitVfSAy7f
Just copy and paste the wallet number when transferring.
If you do not know how to do this - ask Google.
My system automatically recognizes the translation.
As soon as the specified amount is received, all your data will be destroyed from my server, and the rootkit will be automatically removed from your system.
Do not worry, I really will delete everything, since I am 'working' with many people who have fallen into your position.
You will only have to inform your provider about the vulnerabilities in the router so that other hackers will not use it.
Since opening this letter you have 48 hours.
If funds not will be received, after the specified time has elapsed, the disk of your device will be formatted, and from my server will automatically send email and sms to all your contacts with compromising material.
I advise you to remain prudent and not engage in nonsense (all files on my server).
Good luck!

Verzia 8:

Hello!
I'm is very good programmer, known in darkweb as eddie43.
I hacked this mailbox more than six months ago,

through it I infected your operating system with a virus (trojan) created by me and have been spying for you a very long time.
I understand it is hard to believe, but you can check it yourself.
I'm sent this e-mail from your account. Try it yourself.
Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer
and automatically saved access for me.
I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.
I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!
During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!
I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $269 is quite a fair price to destroy the dirt I created.
Send the above amount on my BTC wallet (bitcoin): 1JRCbCH9E3iLhSXPTqtkgfAsJNT2xD74C5
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.
Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!
Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.
I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Verzia 9 – čínsky jazyk:

我问候你！
我有个坏消息。
22/08/2018-在这一天，我攻击了您的操作系统并完全访问了您的帐户 zacek@utb.cz。
就是这样。
在您当天连接的路由器的软件中，存在一个漏洞。
我首先攻击了这个路由器并将恶意代码放在上面。
当您通过Internet输入时，我的木马安装在您设备的操作系统上。
之后，我完成了你的磁盘转储（我有你所有的地址簿，查看网站的历史记录，所有文件，电话号码和所有联系人的地址）。
一个月前，我想锁定你的设备并要求少量资金解锁。
但我查看了您经常访问的网站。你最喜欢的资源令我震惊。
我说的是成人网站。
我想说-你是个大变态者。你有一个令人眼花缭乱的幻想！
在那之后，我想到了一个想法。
我制作了你喜欢的成人网站的截图（你知道我的意思，是吗？）。
之后，我在浏览本网站时拍摄了你和你的娱乐照片（我使用了你设备的相机）。
结果很棒！不要犹豫！
我深信您不想向您的亲戚，朋友或同事展示这些照片。
我认为391美元对于我的沉默是少量的。
此外，我花了很多时间在你身上！
我在比特币接受钱。
我的BTC钱包：1P7bLeCJywaaDRQpT7iwb4qzUHa4CpRFyP
您不知道如何补充比特币钱包？
在任何搜索引擎中写“如何补充btc钱包”。
这很简单。
对于付款，你有两天多一点（恰好50小时）。
别担心，计时器将在您打开此信件时开始。是的，是的..它已经开始了！
付款后，我的病毒和你的妥协自动毁灭。
如果我没有收到您指定的金额，您的设备将被屏蔽，您的所有联系人都会收到您娱乐的照片。

要谨慎！
-不要试图找到并摧毁我的病毒（您的所有数据都已上传到远程服务器）
-不要试图联系我（这是不可能的，我通过您的帐户向您发送了此电子邮件）
- 各种安全服务对您没有帮助;格式化磁盘或销毁设备也无济于事，因为您的数据已经在远程服务器上。
附：我保证，付款后我不会打扰你，因为你不是我唯一的客户。
这是一个黑客的荣誉准则。
从现在开始，我建议你使用好的防病毒软件并定期更新（每天几次）！
不要生我的气，每个人都有自己的工作。
再见

Verzia 10:

Hello!
As you may have noticed, I sent you an email from your account.
This means that I have full access to your account.
I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.
If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.
I also have access to all your contacts and all your correspondence.
Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.
I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.
If you want to prevent this,
transfer the amount of $699 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").
My bitcoin address (BTC Wallet) is: 1Jh1miFmhTmGQvn6Zejaqg85viD4k1vVjG
After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.
Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.
If I find that you have shared this message with someone else, the video will be immediately distributed.
Best wishes!

Verzia 11:

Hello!
I have very bad news for you.
12/10/2018 - on this day I hacked your OS and got full access to your account zacek@fai.utb.cz
So, you can change the password, yes... But my malware intercepts it every time.
How I made it:
In the software of the router, through which you went online, was a vulnerability.
I just hacked this router and placed my malicious code on it.
When you went online, my trojan was installed on the OS of your device.
After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).
A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.
I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!
And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).

After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!
I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $654 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!
Pay ONLY in Bitcoins!
My BTC wallet: 145SmyE7DBEQExsnXZobojbQqr5UdgbCHh
You do not know how to use bitcoins?
Enter a query in any search engine: "how to replenish btc wallet".
It's extremely easy
For this payment I give you two days (48 hours).
As soon as this letter is opened, the timer will work.
After payment, my virus and dirty screenshots with your enjoys will be self-destruct automatically.
If I do not receive from you the specified amount, then your device will be locked, and all your contacts will receive a screenshots with your "enjoys".
I hope you understand your situation.
- Do not try to find and destroy my virus! (All your data, files and screenshots is already uploaded to a remote server)
- Do not try to contact me (this is not feasible, I sent you an email from your account)
- Various security services will not help you; formatting a disk or destroying a device will not help, since your data is already on a remote server.
P.S. You are not my single victim. so, I guarantee you that I will not disturb you again after payment!
This is the word of honor hacker
I also ask you to regularly update your antiviruses in the future. This way you will no longer fall into a similar situation.
Do not hold evil! I just do my job.
Have a nice day!

Verzia 12:

I'll begin with the most important.
I hacked your device and then got access to all your accounts... Including zacek@fai.utb.cz.
It is easy to check - I wrote you this email from your account.
Moreover, I know your intim secret, and I have proof of this.
You do not know me personally, and no one paid me to check you.
It is just a coincidence that I discovered your mistake.
In fact, I posted a malicious code (exploit) to an adult site, and you visited this site...
While watching a video Trojan virus has been installed on your device through an exploit.
This darknet software working as RDP (remote-controlled desktop), which has a keylogger,
which gave me access to your microphone and webcam.
Soon after, my software received all your contacts from your messenger, social network and email.
At that moment I spent much more time than I should have.
I studied your love life and created a good video series.
The first part shows the video that you watched,
and the second part shows the video clip taken from your webcam (you are doing inappropriate things).
Honestly, I want to forget all the information about you and allow you to continue your daily life.
And I will give you two suitable options. Both are easy to do.
First option: you ignore this email.
The second option: you pay me $750(USD).
Let's look at 2 options in detail.
The first option is to ignore this email.
Let me tell you what happens if you choose this path.
I will send your video to your contacts, including family members, colleagues, etc.
This does not protect you from the humiliation that you and
your family need to know when friends and family members know about your unpleasant details.
The second option is to pay me. We will call this "privacy advice."
Now let me tell you what happens if you choose this path.
Your secret is your secret. I immediately destroy the video.
You continue your life as if none of this has happened.
Now you might think: "I'll call to police!"
Undoubtedly, I have taken steps to ensure that this letter cannot be traced to me,

and it will not remain aloof from the evidence of the destruction of your daily life.
I don't want to steal all your savings.
I just want to get compensation for my efforts that I put in to investigate you.
Let us hope that you decide to create all this in full and pay me a fee for confidentiality.
You make a Bitcoin payment (if you don't know how to do it, just enter "how to buy bitcoins" in Google search)
Shipping amount: $750(USD).
Getting Bitcoin Addresses: 1GF8J1XRaiX2oHM7SQo9VAFAtWZcRgMncg
(This is sensitive, so copy and paste it carefully)
Don't tell anyone what to use bitcoins for. The procedure for obtaining bitcoins can take several days, so do not wait.
I have a spetial code in Trojan, and now I know that you have read this letter.
You have 48 hours to pay.
If I don't get BitCoins, I'll send your video to your contacts, including close relatives, co-workers, and so on.
Start looking for the best excuse for friends and family before they all know.
But if I get paid, I immediately delete the video.
This is a one-time offer that is non-negotiable, so do not waste my and your time.
Time is running out.
Bye!