Vysoká škola báňská – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra informatiky

Detekce phishingu v elektronické poště
Tools for Email Phishing Detection

2013 Miroslav Souček

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Miroslav Souček**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Detekce phishingu v elektronické poště
Tools for Email Phishing Detection

Zásady pro vypracování:

Cílem práce je vytvořit nástroj pro detekci phishungu v rámci komunikace prostřednictvím elektronické pošty:

1. Seznamte se a vymezte pojem Počítačová kriminalita – průřez trestnou činností, formy počítačové kriminality.
2. Popište forenzní analýzy dat při zjišťování trestné činnosti a zajišťování důkazních materiálů. Popište známé postupy a způsoby shromažďování dat.
3. Popište nástroje pro forenzní analýzy.
4. Na základě teoretických poznatků, proveďte analýzu, návrh a implementaci nástroje pro prevenci phishingu v oblasti bankovnictví prostřednictvím elektronické pošty a odkazujících webových stránek.
5. Implementaci proveďte v jazyce C#.
6. Výsledek implementace nasaďte do zkušebního provozu a popište výsledky testování.
7. Porovnejte s exitujícími filtry nevyžádané pošty aplikace MS Outlook a dalšími nástroji třetích stran.

Seznam doporučené odborné literatury:

[1] Informační kriminalita: http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni.html
[2] Phishing bez záhad, Lance James, 978-80-247-1766-1, GRADA

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Radoslav Fasuga, Ph.D.**

Datum zadání: 18.11.2011

Datum odevzdání: 07.05.2013

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení:

„Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.“

V Ostravě dne 6.5.2013

Podpis:

Poděkování

Děkuji vedoucímu mé bakalářské práce Ing. Radoslavu Fasugovi, Ph.D za jeho vedení, za všechny předané znalosti a všestrannou pomoc, kterou mi věnoval při řešení a sepsání této práce.

Dále bych rád poděkoval své přítelkyni za její morální a duševní podporu a za vytvoření klidného zázemí a svému zaměstnavateli a kolegům za umožnění studia a jejich podporu.

Abstrakt:

Cílem této bakalářské práce bylo vysvětlit problematiku a druhy počítačové kriminality, popsat forenzní analýzy dat při odhalování trestné činnosti a zajišťování důkazních prostředků. Analýza popisovaného problému proběhla na základě teoretických informací získaných z uvedených zdrojů. Návrh a implementace nástroje byly provedeny v jazyce C#. Vytvořený nástroj byl nasazen do zkušebního provozu na několika emailových účtech. Tento provoz ukázal, že nástroj lze úspěšně použít pro odhalení potencionální hrozby phishingu v elektronické poště z oblasti bankovnictví a odkazujících stránek.

Klíčová slova:

Phishing, počítačová kriminalita, forenzní analýza, Email klient, C#, Microsoft Visual Studio 2010

Abstract:

The aim of this bachelor thesis was to explain the problematic and types of cybercrime; also describe forensic data analysis in identification of crime and ensuring of evidence. Analysis of the problem was performed on the acquired theoretical information, design and implementation of a tool was performed in language C#. Created tool was deployed into trial operation on few email accounts. This operation showed that the instrument can be successfully used for detecting potential threats of phishing e-mails from banking area and referring pages.

Key words:

Phishing, Computer crime, forensic analysis, Language C#, Email client, Microsoft Visual Studio 2010

1. Úvod

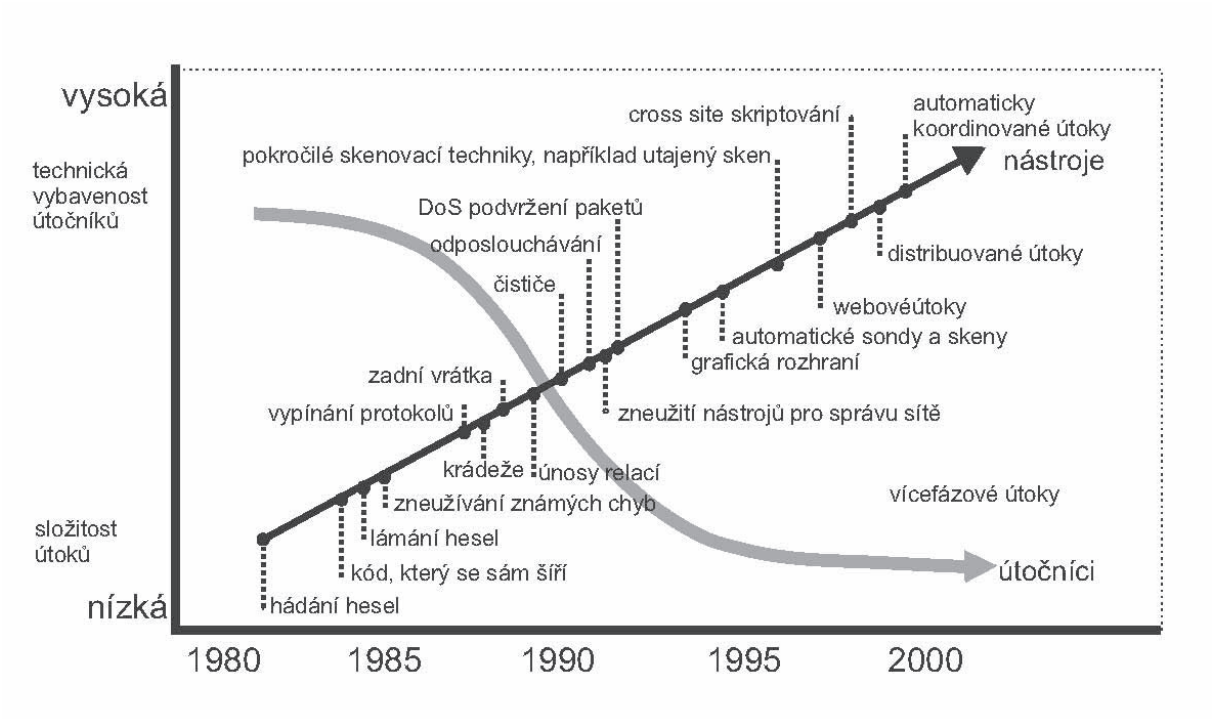
Při rozšíření PC (Personal computer) se začala šířit i počítačová kriminalita a vše co s tímto fenoménem souvisí. Společně s rychlým vývojem výpočetní techniky byl i rychlý vývoj počítačové kriminality. Informační a komunikační technologie postupně pronikali a pronikají do všech odvětví lidské činnosti a staly se její nedílnou součástí. Dnes už si těžko někdo dokáže představit život bez využití výpočetní techniky ať už v jakékoli podobě. V současné době se už také zdaleka nejedná pouze o kriminalitu spojenou čistě jenom s PC, ale často se jedná o na první pohled zcela odlišnou trestnou činnost, v které se až postupnými kroky v důkazním řízení zjistí přítomnost důležitých skutečností spadajících do tohoto odvětví. Je to zapříčiněno oním neoddiskutovatelným pronikáním výpočetní techniky do lidského bytí ve všech jeho podstatách. Právě toto, samozřejmě společně s globálním využitím a rozmachem všech moderních technologií, přináší i obrovský rozmach řady negativních jevů. V zájmu sjednocení roztříštěné a nekompatibilní legislativy evropských států, která čelila neustále rostoucímu zájmu potencionálních pachatelů o tento druh trestné činnosti, přijala Rada Evropy[1] členění počítačové kriminality. Z této úmluvy vychází pojmově, co se týče počítačové kriminality i nový trestní zákon. Úmluva obsahuje souhrn aktivit, které by smluvní strany měly v rámci svého práva postihovat jako trestné činy. Jedná se o tyto aktivity:

- ✓ Hlava1: trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů
  - ➢ neoprávněný přístup,
  - ➢ nedovolené sledování,
  - ➢ narušování dat,
  - ➢ narušování systémů,
  - ➢ zneužití zařízení,
- ✓ Hlava 2: počítačové trestné činy související s
  - ➢ padělání související s počítači,
  - ➢ podvod související s počítači,
- ✓ Hlava 3: trestné činy související s obsahem dat
  - ➢ trestné činy související s dětskou pornografií,
- ✓ Hlava 4:trestné činy související s porušením autorského práva
  - ➢ trestné činy související s porušením autorského práva a práv s ním související

[1] Úmluva o počítačové kriminalitě, schválené Výborem ministrů Rady Evropy 8. 11. 2001, Česká republika tuto Úmluvu podepsala v roce 2005, avšak dosud neratifikovala, stejně jako ji neratifikovala přibližně polovina dalších členů Rady Evropy.

- ✓ Hlava 5: doplňková odpovědnost a sankce
  - ➢ pokus, napomáhání a účastenství
  - ➢ sankce a opatření

Se zvyšující se dostupností výpočetní techniky a internetu se také zvyšuje vzdělanost pachatelů a tím i složitost jejich útoků. Skupina CERT[2] provedla v roce 2002 studii o kyberterorismu týkající se určité části počítačové kriminality a ta ukázala, že útočníci jsou čím dál chytřejší a mají k dispozici i lepší vybavení. Teoreticky se dá říci, že závěr studie byl o praktické nezastavitelnosti útočníků, viz obrázek 1. [1], [2], [6]



Obr. 1 Rafinovanost a znalosti hackerů stoupají [2]

V zájmu celé společnosti je tedy se proti těmto negativním jevům provázejícím počítačový boom účinně bránit a činit opatření k zamezení jejich šíření. Tyto obranné kroky jsou prováděny buď preventivně, nebo represivně. Mezi preventivní opatření patří hlavně snaha zabránit vzniku narušení integrity a zabezpečení. Mezi represivní opatření patří již samotné odhalování, vyšetřování a následné potrestání trestné činnosti vznikající v souvislosti s veškerou činností, která je jako trestný čin stanovena v zákoně. Je samozřejmé a dle platné legislativy i nutné, k vypátrání a následnému potrestání pachatele či pachatelů posbírat důkazy, které směřují a usvědčují fyzické osoby z dané činnosti. Jedna z metod, která slouží k získávání a shromažďování důkazů týkajících se počítačové

[2] Organizace CERT Coordination Center (CC) je státem založená a financovaná – vznikla v roce 1988 v USA jako reakce na první velký internetový virus.

kriminality, se nazývá forenzní analýza dat, vědní obor, který zasahuje i do spousty dalších odvětví nejen spojených s počítačovou kriminalitou. [3]

Nástroje, používající se k této analýze dat se nazývají „Forenzní analyzátory“. Tyto můžeme dále rozdělit na analyzátory:

- hardwarové
- softwarové

Hardwarové analyzátory nejčastěji zjišťují data na nejnižší analogové úrovni, tedy přímo z pevného disku. Jejich rozlišovací schopnost pro kvalitní zpracování musí být tedy vyšší, což má dopad i na pořizovací cenu. Oproti těmto stojí softwarové analyzátory, které jsou implementovány na speciálně upravených PC, ke kterému se připojí analyzované medium. Toto je obvykle realizováno přes rozhraní, které zamezuje jak poškození media, tak změně či zápisu na hardwarové či softwarové úrovni z důvodu nežádoucí změny na zkoumaném mediu.

Vlastní proces probíhající v rámci forenzní analýzy lze rozdělit na několik stádií, kterými musí projít:

- Získání dat ke zkoumání (zajištění datových nosičů na místě činu při dodržení určitých pravidel, viz níže)
- Analýza (vlastní forenzní analýza datových nosičů příslušným nástrojem)
- Report (výstupní informace, které jsou přesně zadokumentovány)

Tato práce se nezabývá podrobně celým cyklem forenzní analýzy, ale pouze průřezem této velmi náročné vědní disciplíny se zaměřením na část, která účelově neoprávněně získává data od uživatelů za účelem jejich shromažďování a následného dalšího zneužití.

2. Obecná část

2.1. Základní definice názvosloví

2.1.1. Forenzní analýza

Forenzní analýza dat používaná pro odhalování a vyšetřování počítačové kriminality se přímo zabývá sbíráním, zajišťováním a následným zkoumáním digitálního důkazního materiálu použitelného pro trestní řízení. Jde o využití vědecky odvozených metod. Jedná se jak o pevné disky, tak i veškerá paměťová media jako jsou CD, DVD, Flash disky, paměťové karty apod. Pro vlastní zajištění důkazů jsou tato media podrobena analýze zaměřené na jejich obsah. Odhalují se a identifikují se data, která by mohla souviset s vyšetřovanou nelegální činností. K tomuto se velmi často používají principy a metody podobné těm, které se používají pro obnovu dat. U takto získaných dat se musí provést samotná analýza obsahu, tedy souborů a složek, které můžou vést k dalšímu získání informací (např. analýza obrázků, videí, zvukových záznamů, ale i textových souborů, HTML dokumentů apod.). Takto získané a zadokumentované skutečnosti se nakonec zpracují do závěrečné zprávy tzv. reportu.

2.1.2. Počítačová kriminalita

K běžně používanému výrazu pro tento druh trestné činnosti řadíme vedle již zmíněné počítačové kriminality také *„kriminalitu informačních technologií“* a *„kriminalitu elektronickou“*. V zahraničních pramenech se můžeme setkat s anglickým ekvivalentem tohoto pojmu – *„cybercrime“*, *„hightech-crime“*, *„IT crime“*, či v neposlední řadě *„computer crime“*.

Pojem počítačová kriminalita nemá žádný oficiálně definovaný obsah. Je třeba ji chápat jako specifickou trestnou činnost, kterou je možné páchat s pomocí výpočetní techniky, kde je výpočetní technika předmětem trestného činu, nebo pachatelovým nástrojem použitým ke spáchání trestného činu. Aby bylo možno hovořit o počítačové kriminalitě, nestačí pouze vlastní užití počítače, ale jednání pachatele musí naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoně a jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost. [1]

Základní hrozby spadající do počítačové kriminality můžeme rozdělit do čtyř skupin, které odrážejí čtyři hlediska bezpečnosti informačního systému

- Únik informace (jde o případ, kdy je důvěrná informace sdělena neautorizovanému subjektu, nebo je tímto subjektem odhalena. Toto může vést k přímým útokům se značnými následky).

- Narušení integrity (jedná se o porušení konzistence dat, kdy může dojít k vytvoření dat nových či změně nebo vymazání dat stávajících neautorizovaným subjektem).
- Potlačení služby (jde o úmyslné bránění přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům. Jako příklad mohou posloužit známé útoky DoS, kde dochází k úmyslně vysoké zátěži zdroje jalovými a nelegitimními žádostmi. Toto vede k neúspěšným pokusům o přístup ze strany legitimních subjektů).
- Nelegitimní použití (jde o úmyslné použití informačního systému jiným než oprávněným uživatelem). [5]

2.1.3. **Digitální stopa**

Mezi prvními ve druhé polovině 80. let minulého století vznikl spolu s pojmem „počítačová kriminalita“ pojem „počítačová stopa“. U tohoto pojmu nenalezneme přímou definici, jelikož se jedná spíše o intuitivní používání, to je v dnešní době nedostatečné, protože i jiná elektronická zařízení zanechávají stopy, které mají stejnou podstatu, charakter a obecné nebo individuální vlastnosti jako stopa počítačová. Proto, pokud se rozhlédneme po světové literatuře, najdeme zde několik podobných definic, které vymezují již vžitý termín „digitální stopa“ (digital evidence).

Nejčastěji používaná definice v literatuře je definice, jež byla navržena již v roce 1999 pracovní skupinou SWGDE – Scientific Working Group on Digital Evidence[3]:

„Digitální stopa je jakákoli informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“

Takto je definice použitelná u jakékoli digitální technologie. Digitální stopa daná touto definicí může pokrýt jak oblast počítačů a počítačové komunikace, tak i oblast digitálních přenosů, videa, data kamerových (CCTV) systémů a jiných technologií potencionálně spojených s high-tech kriminalitou. Tato definice digitální stopy je do značné míry obecná, což je velmi důležité pro odstranění milné představy, že digitální stopa je spjata pouze se spácháním trestného činu. Digitální stopa musí být využitelná nejen pro kriminalistiku a orgány konajícími v trestním řízení, ale i pro forenzní šetření prováděné státními orgány (občanskoprávní spory, obchodní zákony, apod.) a šetření prováděné na komerční bázi (nezávislé audity jak interní, tak externí) apod.

Původně byla digitální stopa definována organizací International Organization of Computer Evidence (IOCE) jako jakákoli informace přenášena nebo uchovávána v binární formě, která

[3] skupina SWGDE byla založena z iniciativy FBI v roce 1998. Prvních jednání pracovní skupiny se účastnili zástupci Bureau of Alcohol, Tobacco and Firearms (ATF), U.S. Customs, the Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA), U.S. Secret Service (USSS) a U.S. Postal Inspection Service. Postupně docházelo ke slaďování projektu s International Organization on Computer Evidence (IOCE) a Interpolem

může být předložena soudu jako věcný důkaz. Jelikož však v praxi při forenzních šetřeních, prováděných ať už firmou či fyzickou osobou zabývající se přímo forenzní analýzou, nemusí být výsledek předkládán soudu, ale výsledky směřují spíše k managementu firmy či akcionářům, není tato definice zcela vhodná. Proto by pojem digitální stopa (stejně jako jakákoli jiná stopa) měl být nasměrován jen na průběh vyšetřování a svou podstatou standardizovat nejen postupy, ale i používané pojmy. To by mělo platit pro jakýkoli vyšetřující orgán a tím zaručit přenositelnost stop i vyšetřovacích metod mezi různými účastníky šetření. (Např.: Pokud audit ve firmě poskytovaný externí auditní firmou zjistí spáchání trestného činu, musí být zaručeno předání důkazů spolu s metodami orgánům činným v trestním řízení v takové podobě, v které bude možné v analýze pokračovat bez nutnosti konvertovat do jiných formátů.)

2.1.4. **Kyberprostor**

Tento termín, v České Republice používán i anglický název cyberspace, se používá pro označení virtuálního světa vytvářeného počítači, telekomunikačními sítěmi apod. paralelně s „reálným" světem. Jde o virtuální svět vytvořený moderními technologickými prostředky. Je používán především lidmi pracujícími s počítači a internetem a je navíc zmíněn v oficiálním názvu Úmluvy o počítačové kriminalitě (Convention on Cybercrime)[4]. Kyberprostorem je myšlena i oblast počítačových systémů a sítí, v níž jsou ukládána data a v níž probíhá on-line komunikace. V základě jde o síť, neidentifikovatelný prostor mezi počítači, mezi modemy, neurčitý prostor, kde se každodenně odehrává veškeré dění na síti jako je zábava, komunikace, obchod a samozřejmě i zločiny. V této oblasti počítačové kriminality jsou nejvíce ohroženy činnosti v souvislosti s Internetem, potažmo s „World Wide Web". V dnešní době je počítačová kriminalita, která souvisí s internetem samostatnou kategorií, která pomalu vlastní počítačovou kriminalitu, která nesouvisí s Internetem, ať už přímo nebo nepřímo, zatlačuje do pozadí, jelikož i pachatelé od ní pomalu ustupují.

2.2. **Příklady počítačové kriminality**

- ✓ Sabotáže – pravděpodobně první čistě počítačový zločin se u nás odehrál v 70. letech minulého století, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách.
- ✓ Dokladové delikty – typickým příkladem je podvod v zásilkovém obchodě MAGNET, kdy pracovnice odebírala zboží na adresu své matky a do databáze odběratelů vždy uvedla, že zboží bylo zaplaceno.

[4] Convention on Cybercrime (Budapest, 23.11.2001)

- ✓ Neoprávněné užívání počítačů – klasickým zahraničním případem je odsouzení hackera za krádež elektrické energie, kterou spotřeboval neoprávněným užíváním počítače.
- ✓ Padělky – např. grafické počítačové systémy pro elektronickou sazbu a grafickou úpravu publikací, tzv., Desk Top Publishing – s tímto nástrojem zhotovovali pachatelé v několika rozsáhlých sítích obchodníků s kradenými automobily falešné technické průkazy a jiné doklady. Byly použity i pro zhotovení falešných cenných papírů a jiných bankovních dokumentů.
- ✓ Bankovní počítačové podvody – v roce 1994 se odehrál případ, který upozornil na nebezpečnost novodobých počítačových „pirátů“, formujících se do skupin. Ruská hackerská skupina vedená Vladimírem Levinem pronikla do počítačové sítě Citibank a převedla na své účty částku deset miliónů dolarů. Přestože v krátké době došlo k odhalení a dopadení pachatelů, můžeme tento jejich čin brát jako skutečně zlomový v dějinách počítačové kriminality, který nastavil nový směr počítačového zločinu. V českém bankovním sektoru došlo k několika bankovním počítačovým zločinům. Všechny spáchané trestné činy pomocí počítače měly charakter neoprávněné manipulace s bankovními záznamy (účty, hlavní knihou, souborem převodních příkazů apod.) a byly kvalifikovány jako podvody dle trestního zákona.
- ✓ Porušování autorských práv – dva druhy duševního vlastnictví – oba spadající pod ochranu autorským zákonem – se staly masivním předmětem útoku pachatelů: audiovizuální nahrávky a počítačové programy.
- ✓ Extremismus – internet se stal skvělým prostředkem a pomocníkem různých extrémistických skupin operujících jak po celém světě, tak v České republice. Určitě si sem můžeme zařadit nechvalně známé neonacisty, anarchisty, komunisty, militantní náboženské sekty, radikální ekologické skupiny a mnohé dalších.
- ✓ Počítačové viry – zde je počítačový zločin, o kterém se převážně nejčastěji mluví a píše, vlastní infikování PC počítačovým virem. V poslední době byly rozšířeny velmi nebezpečné viry a tzv. makroviry, kdy v některých případech byl dokonce dopaden a trestně "odstíhán" jejich autor.
- ✓ Ilegální sbírání osobních údajů, nosičů informací, dat a jejich zneužívání – konkrétní případ zneužití, kdy zdravotní personál poskytl seznam pacientů s diagnózou rakoviny distributoru léčiv.

2.3. Formy počítačové kriminality

2.3.1. Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů

- Hacking

Vedle porušování autorských práv je tento druh počítačové kriminality zabývající se pronikáním do systémů jednou z nejvýraznějších oblastí. Základem je průnik do systému jinou než standardní cestou, tedy prolomení, nebo jiné obejití zabezpečení. Ti nejlepší hackeři se vyvíjejí z programátorů snažících se zjistit, jak systém funguje, popřípadě odstranit chyby a tím se něco nového přiučit. Hackery můžeme dělit dle jejich činnosti do dvou základních skupin. První, která svou činností nemá v úmyslu cílový systém jakkoli poškodit a bere toto jako adrenalinovou zábavu, kde zkouší, co dokáže a učí se tímto nové věci a druhou skupinu, která sleduje pouze materiální cíle.

Ve světě hackerů můžeme rozlišit několik typů hackerů:

- Wannabes – občas označováni jako tzv. Lameři (trapní snaživci). Nejsou bráni jako skuteční hackeři. Jde o nejníže postavenou skupinu, jejíž členové, aniž by znali jakýkoli programovací jazyk, samy neprogramují, pouze spouštějí předpřipravené hackerské programy (odtud i jejich označení Wannabes – volně přeloženo „rádoby hacker“). Ostatní hackeři tuto skupinu ignorují. Činnost těchto lidí je dle trestního zákona posuzována naprosto stejně jako u ostatních skupin.
- White hats – tzv. „Hodní hackeři“, kteří uznávají a řídí se hackerskou etiku. U této skupiny se dá do jisté míry hovořit o následovnících odkazu původních hackerů. Tito hackeři své útoky provádí za účelem nového poznání a nikoli za účelem páchání škody na napadených systémech. Podskupinou jsou tzv. „Samurajové“. Tito po samotném útoku kontaktují správce, například pomocí e-mailu ze superuživatelského accountu a informují ho, jak a kudy došlo k napadení a jak tuto díru v zabezpečení vyplnit. Někdy bývají tito lidé najímáni firmami k účelnému napadání jejich produktu k odstranění oněch děr a slabin ještě před uvedením do provozu. Toto poté není klasifikováno jako trestný čin.
- Black hats – skupina, která svou činnost staví na majetkovém nebo jiném prospěchu. Jejich nabourávání do systému má většinou za následek jeho poškození, ztrátu nebo změnění dat. Bývají označováni též jako Crackers.
- Grey hats – skupina hackerů, kteří stojí na pomyslné hranici mezi bílými a černými. Jde o předpokládanou skutečnost, že i „bílí hacker“ může někdy spáchat trestně postihnutelný čin spjatý s počítačovou kriminalitou a naopak „černý hacker“ se může stát po odpykání trestu, nebo i bez odhalení, bezpečnostním expertem, kde využije své znalosti. [2]

Dále do této skupiny spadá tzv. „hacktivismus“ což je politicky motivovaný útok na internetové stránky. V tomto rozvíjejícím se odvětví nejsou již zapojení pouze jednotlivci a organizované skupiny, nýbrž se sem zapojují pravděpodobně i odborníci a profesionálové z různých tajných služeb jednotlivých států. Jako například útoky na webové servery izraelského Parlamentu a ministerstva zahraničí. Dále byly pravděpodobně izraelskou tajnou službou opakovaně napadeny na Blízkém východě webové stránky fundamentalistického hnutí Hizballáh, na stránky Hamasu bylo např. umístěno tvrdé porno. Z nedávné historie o praktikách a vyžití těchto služeb vypovídá uniklá studie, která ukazuje, jak Pentagon dostává rady od soukromých firem ohledně kybernetických sabotáží vůči Libyi. Studie (Project Cyber Dawn) byla diskutována v e-mailech, ke kterým se dostala skupina LulzSec. Byly ukradeny z firmy zabývající se internetovým dohledem (Unveillance).

V České republice jsme se s tímto setkali například při napadení stránek KSČM v roce 2012 po vyhlášení výsledků krajských voleb, kde získali nejvíce mandátů od převratu. Webové stránky brněnské pobočky strany napadli hackeři za skupiny Anonymous. Toto ale nebyl první ani jediný útok. Předtím byli např. stránky lidovců, které 12. 6. 2002 napadl hacker vystupující pod přezdívkou EB#L@. Potvrzením, že se jednalo v tomto případě opravdu o hacktivismus byl e-mail, který útočník zaslal administrátorovi serveru s tím, že chtěl pouze vyjádřit svůj politický názor.

- Sniffing

Jedná se o metodu odposlouchávání počítačové sítě, tedy přesněji provozu na počítačové síti. Zachycené pakety přenášející se po síti mohou nést důvěrné informace, které lze dále zneužít například v hackingu, nebo ve formách klasické trestné činnosti. Možnost získání nešifrované komunikace ze sítě je v dnešní době neuvěřitelně jednoduchá. Na internetu je celá řada volně šiřitelných nástrojů na odposlech sítě (např. dsniff, Ethereal, WireShark apod.), k jejichž použití není potřeba speciálních znalostí.

V souvislosti se Sniffingem je samozřejmě nejznámější problematika elektronické pošty. Na tuto se stejně jako na jinou soukromou komunikaci po síti vztahuje listovní tajemství a tedy je nedotknutelná. Při komunikaci počítače se serverem bez šifrování je odesílaná adresa a následně i heslo viditelné pro každého, kdo je v tu chvíli připojen k síti a odchytává komunikaci. Počítač přijímá data určená pouze jemu, protože ho od zbytku sítě dělí hardwarová vrstva v podobě síťové karty, ale bohužel téměř každá síťová karta jde přepnout do tzv. „promiskuitního“ režimu, kdy se filtr vypne a karta pouští do systému naprosto vše.

- Narušování dat

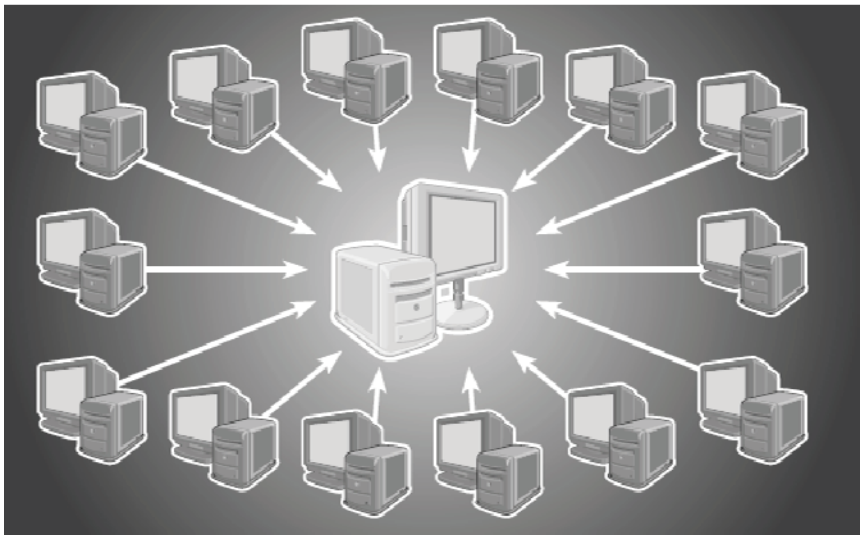
V tomto případě dochází k nelegálnímu zásahu do dat a to ve většině případů po napadení hackerem či útoku crackera. Je zde vždy sledován určitý konkrétní cíl, kde názorný příklad najdeme u crackingu prováděného na různých softwarech. Základním cílem je odstranění ochrany, obejití licenčních podmínek a to tím, že je vytvořen crack, který umožní nelegální užívání softwaru a jeho následné šíření a užívání dalšími uživateli. V případě hackerského útoku je typickým příkladem narušování dat poškození, pozměnění nebo zablokování webových stránek cílových skupin. Jde tedy o získání neoprávněného přístupu k datům a jejich zneužití, pozměnění, nebo dokonce zničení. V tomto případě tedy jde o nelegitimní získání přístupu k datům a neoprávněnou manipulaci s nimi.

- Narušování systémů

Do této skupiny kybernetických útoků řadíme především ty, které mohou závažným způsobem narušovat funkčnost informačních systémů . Především sem patří DoS (Denial of Service) útoky, které zapříčiňují odmítnutí služby, tzn., snaží se o znepřístupnění některé určité služby, počítače, nebo i sítě. Myšlenka je taková, že pokud nemohu napadnout přímo stroj, je jeho slabinou spojovací cesta. Nejedná se tedy přímo o neoprávněný zásah do počítače, ale o zahlcení síťové komunikace, kdy je počítač úplně vyřazen, nebo je znatelně snížen jeho výkon. Je několik základních metod útoku DoS:

- zahlcení odesíláním jalových paketů z více počítačů. Tento způsob se nazývá DDoS (Distributed Denial of Service), (viz Obr. 2)
- zahlcení sítě cílového počítače příkazem ping
- zahlcení volných systémových prostředků

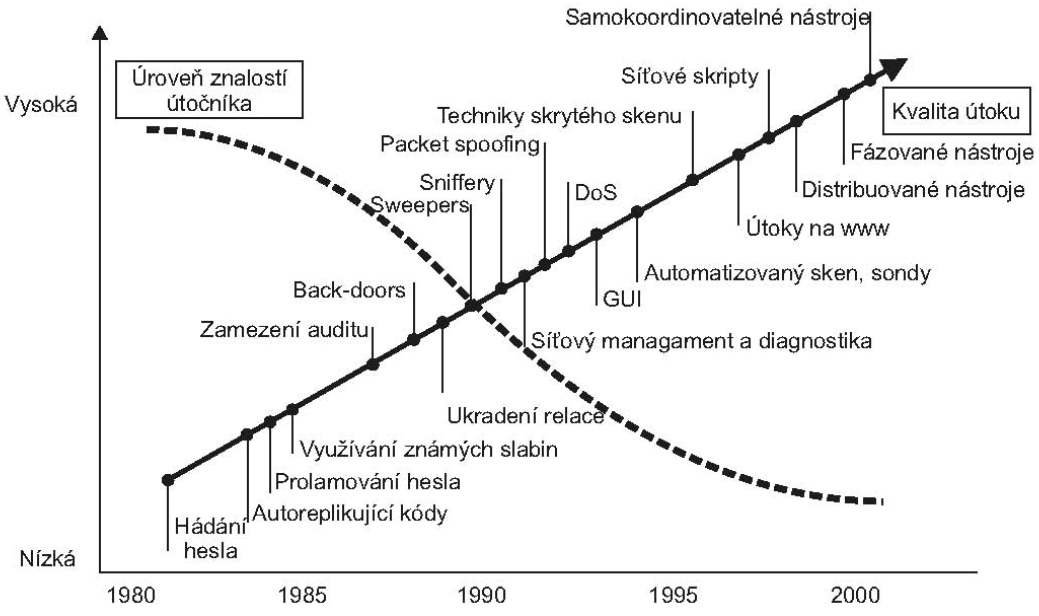
Kromě útoků DoS a DDoS jsou od těchto odvozeny i další způsoby útoků jako je například potlačení přístupu DoA (Denial of Access). [5], [12]



Obr. 2 Útok typu DDoS spočívá v tom, že tisíce nakažených počítačů (zombie) poslechnou "svého pána" a v jediném okamžiku zahltí cílový počítač. [12]

2.3.2. **Zneužívání zařízení**

S postupujícím vývojem výpočetní techniky a zabezpečovacích zařízení, metod a softwarů se samozřejmě zdokonalují i ti, kteří usilují o nelegální zneužívání těchto zařízení ať už z jakýchkoli důvodů. (Obr. 3) Používají k tomu dva druhy nástrojů, hardwarové a softwarové.



Obr. 3 Historie vývoje hackerských nástrojů [5]

- Hardwarové nástroje - jako první jím byl tzv. blue-box, který vznikl k oklamání telefonní sítě AT&T. S pomocí této krabičky bylo možné telefonovat zadarmo. Principem mechanismu oklamání telefonní sítě AT&T byl tón o kmitočtu 2,6 kHz, kterým bylo řízeno přepínání dálkových hovorů. Ve Spojených státech v té době vznikla kolem tohoto hardwarového nástroje skupina hackerů, která byla označována jako "phreakers".
- Softwarové nástroje - s postupem času a s vývojem výpočetní techniky jsou softwarové nástroje nejpoužívanější a nejrozšířenější. Jedná se o všechny níže uvedené nástroje:

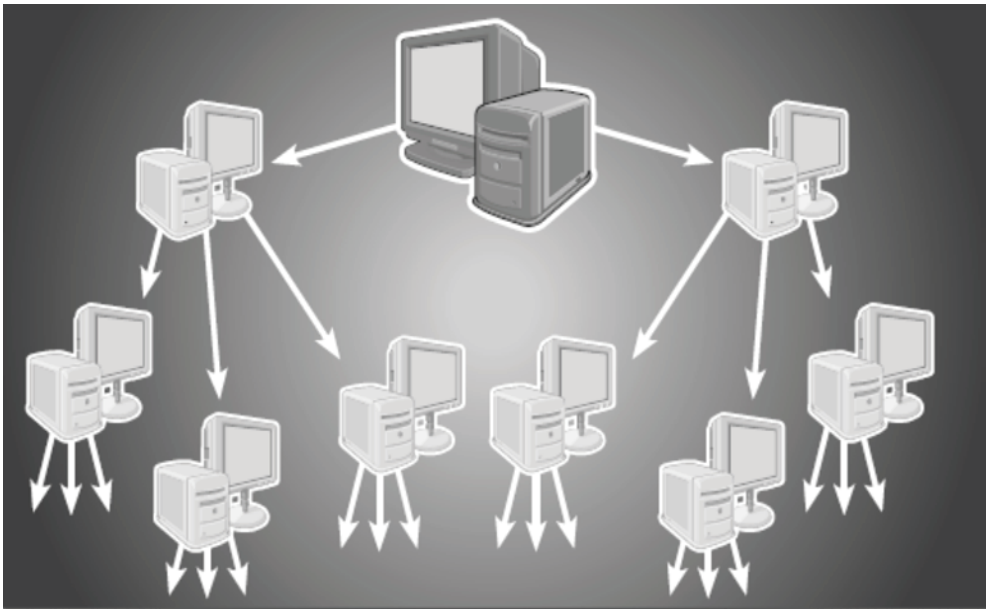
  - Prolamovače hesel - slouží, jak už samotný název říká, k prolomení hesla, tedy ochrany nebo autorizace. Toto prolomení se provádí tím, že použitý nástroj dosazuje různé kombinace znaků, které mohou být dle autora nástroje součástí hesla. Pokud projde autorizace, prolamovač automaticky odesílá heslo hackerovi. Prolamovače dělíme na dva základní druhy:

    - slovníkové útoky (dictionary attack) - používá slova ze své vlastní databáze slov
    - útoky hrubou silou (brute - force attack) - generuje všechny kombinace znaků

  - Backdoor - kódy, pro které je českým ekvivalentem slovní spojení "zadní vrátka", umožňují po jejich instalaci na cílový počítač jeho skryté ovládání a řízení. Jde o jeden z oblíbených hackerských nástrojů. Jakmile hacker odhalí díru v zabezpečení, nainstaluje do stroje backdoor. Většinou mívá v záloze více takových strojů, kde vlastní útoky na cílový stroj provádí přes řetěz těchto upravených počítačů a tyto ho izolují a chrání před případným odhalením.
  - Skener - slouží pro zjištění služeb běžících na otevřených portech počítače. Nejedná se tedy přímo o nástroj určený k útoku na počítač, ale spíše ke sběru informací podobně jako Sniffer a může být předzvěstí potencionální připravovaného útoku.
  - Malware - je společný název pro skupinu škodlivých kódů, které mají za úkol poškodit či zneužít data, nebo poškodit či zneužít počítač.
  - Viry - tento druh škodlivého softwaru již není rozšířen v takové míře, jak tomu bylo dříve. Jedná se o kódy, které po instalaci do počítače infikují co nejvíce souborů, aby zabezpečili své šíření při kopírování souborů a přenosu do dalšího PC. Tento druh infikace byl nejvíce rozšířen v dobách disket, kdy veškeré přenosy dat byly realizovány tímto mediem. V dnešní době, více než aby škodili v napadených počítačích, mají jako hlavní úkol udělat z počítače tzv. otroka nebo zombie. Tímto způsobem může autor viru bez vědomí majitelů počítačů připojených k internetu po celém světě vytvořit obrovskou počítačovou síť vzájemně propojených strojů, takový jeden velký superpočítač, kterému se říká botnet. Tyto se poté dají využít k různým aktivitám, jako například rozesílání e-mailů (spamu) nebo DDoS útokům. [12]

- Červy - jsou modernějšími následníky klasických virů. Hlavní rozdíl je v jejich způsobu šíření. Červ k tomu může využít internetovou síť, kde se kupříkladu samovolně rozešle jako příloha e-mailu všem kontaktům uvedených v poštovním klientovi na infikovaném počítači. Vzhledem ke zdokonalujícím se malwarovým filtrům na poštovních serverech nerozesílá své kopie, ale rozešle pouze odkaz na své umístění. Tyto rozesílá nejen emailem, ale i přes ICQ, SKYPE a podobně. O kliknutí na tento odkaz, tedy nalákání uživatele, je postaráno nějakým zajímavým textem, který má zaujmout. Tomuto se říká sociální inženýrství.

  V současné době se červy šíří i přes paměťová media, jako například Flash disk, kam se škodlivý software zkopíruje. Ten následně na flash disku upraví soubor autorun.inf a tím u většiny počítačů bude stačit pouhé připojení USB.
- Trojský kůň - jeden z nejoblíbenějších hackerských nástrojů současnosti. Jedná se převážně o malý program, který je zabalený do volně stažitelné utility, nové bezplatné hry a podobně. Po rozbalení v počítači mají velké využití od monitorování činnosti prováděné na cílovém počítači až po zneužití počítače k DoS útokům.

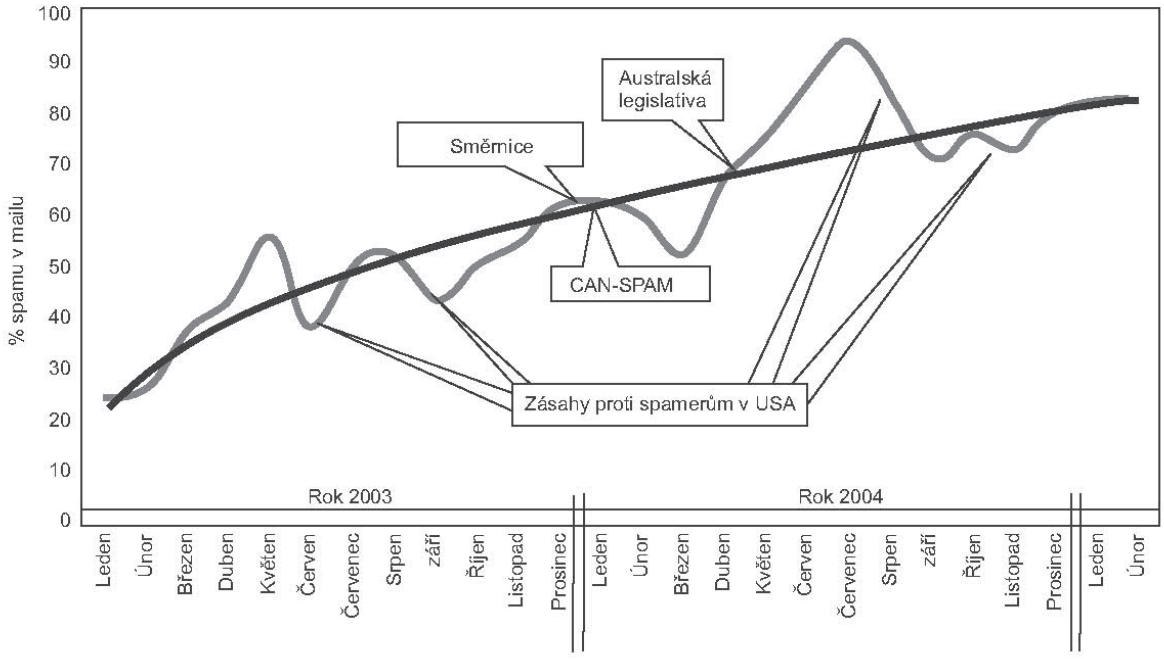


Obr. 4 Počítačové červy se šíří lavinově po internetu - za krátkou dobu mohou nakazit obrovské množství počítačů [12]

- Spyware - jedná se o software, který se samovolně nainstaluje do cílového počítače bez informace uživateli, že se tak děje. Po jeho instalaci se nemusí tento škodlivý software nijak projevovat, ale může mít vliv na funkčnost počítače. Jedná se o sledování online aktivit na síti, sbírání informací, které uživatel zadává, včetně

důvěrných informací, může měnit nastavení počítače, nebo také způsobit jeho zpomalení. [11]

- Adware - určitý druh malwaru, který ale na rozdíl od spywaru není instalován do počítače bez vědomí uživatele a není ani tak škodlivý, jelikož nesbírá data a ani je nikam neodesílá. Jedná se o software, který přímo či nepřímo podporuje reklamu šířenou po internetu, ať už formou obyčejných bannerů, nebo neustále vyskakujícími pop-up okny. Adware si do počítače většinou uživatel instaluje sám přijetím licenčních podmínek u nějakého freewarového programu, v kterých je instalace tohoto malwaru podmínkou pokračování instalace.
- Dialer - je škodlivý software, který v dnešní době patří spíše do malwarového muzea. Je to dáno tím, že tento druh softwaru se zaměřoval u vytáčeného internetového připojení na jeho přesměrování na drahé linky, samozřejmě bez vědomí uživatele.
- Spamming - jde o rozesílání nevyžádané elektronické pošty, většinou reklamního charakteru. Tento způsob nepřímého marketingu může velmi obtěžovat zaplňováním emailové schránky a při archivaci zpráv i pracností roztřídění pošty. Adresy elektronické pošty jsou spammery získávány nejen z různých registrací v síti internet na služby zdarma, ale i z ICQ a podobných komunikačních aplikací. Nárůst spamu je nezadržitelný i když spousta opatření směřují k jeho potlačení, nebo alespoň regulaci.



Obr. 5 Trend ve vývoji spamu [5]

- Sociální inženýrství

Toto slovní spojení je v dnešní době využíváno ve spojení s podvody, nebo podvodným jednáním za účelem získání prospěchu pro sebe nebo třetí osobu. Sociální inženýrství je využíváno skoro u všech malwarů, kde je potřeba získat od uživatelů přístup do počítače, data, nebo jiné citlivé informace. Využívá se zde chyby úsudku jedince. Jedná se například o nalákání uživatele, aby klikl na odkaz v elektronické poště, kde je připraven ke stažení škodlivý malware. Jedná se pouze o to, zaujmout. Poměrně úspěšně jsou používány aktuální události z celého světa. Může jít o zprávy ze společenského života přes teroristické útoky, až po narození potomka slavné celebritě. Nemusí se vždy jednat o skutečné události, jenom musí uživatele zaujmout natolik, aby zvědavost zvítězila nad opatrností. Například se v elektronické poště objeví odkaz, který slibuje video s nahou celebritou. Po kliknutí na tento odkaz se ovšem místo videa zobrazí výzva ke stažení kodeků či přehrávače potřebného k přehrání onoho videa. Jakmile uživatel souhlasí se stažením těchto souborů, otevře dveře svého počítače malweru. Sociální inženýrství je základním kamenem při využívání phishingu. [12]

2.3.3. **Phishing**

Tento druh nelegální činnosti směřuje ke sběru důvěrných informací převážně prostřednictvím elektronické pošty. Tento termín vznikl z anglického slova "rybaření", protože se skutečně jedná o zkoušení nachytání uživatelů na tyto hromadně rozesílané podvodné emaily, přes které se snaží phishers získat citlivá data jako jsou jméno, adresa, číslo platební karty, číslo bankovního účtu, přihlašovací jméno a heslo a podobně. [10]

Tabulka 1 Srovnání phishingového e-mailu a malware [10]

	Phishingové e-maily	Phishingový malware/key loggers
Průměrný týdenní počet napadených účtů	100	500 000
Typ prozrazených údajů	Jméno, adresa, telefon, platební karta, údaj VCC2, číslo bankovního účtu, přihlašovací jméno a heslo, příjmení matky za svobodna, odpověď na ověřovací otázku např. "Zapomněli jste heslo?" Oběť většinou poskytne veškeré požadované informace	Přihlašovací jméno k účtu nebo číslo platební karty s datem expirace a adresou. Jediná oběť většinou přijde o jediný okruh informací. Málo obětí ztratí více než jeden typ informace. Prozrazená informace nemusí odpovídat informaci, kterou phisher potřebuje.
Objem generovaných dat	Jedna oběť generuje zhruba 500B. Týdně se takto zpravidla generuje max. 50kB. Tato data může jediná osoba zpracovat během několika minut.	Jediný trojský kůň pro key- logging trojan může generovat stovky MB dat týdně. Data se nezpracovávají ručně, ale k filtraci se používají skripty. Díky tomu se často ztratí potencionálně cenné informace. Nové druhy malwaru jsou inteligentnější a zpracovávají data přímo z trojského koně jako takového.
Jak dlouho metoda vydrží?	Zpravidla se v neměnné podobě opakovaně používá týdny až měsíce. Provedením drobných změn v adresářích je možno obesílat různé osoby - informace se od téže osoby nezískává dvakrát.	Většina druhů malwaru je účinná týden předtím, než dodavatel antivirového softwaru vytvoří kódy. Některé z phishingových skupin používají malware v omezených množstvích. Tyto programy vydrží mnohem déle, obecně však sklidí méně informací. Jedna osoba, jejíž počítač je nakažen, může stejnou informaci prozradit opakovaně.
Celkové investiční náklady phishera	Vytvořením jednoho phishingového serveru trvá většinou jeden týden. Server lze potom aplikovat na stovky anonymních schránek a opakovaně je používat celé týdny i déle. Změna obsahu phishingového e-mailu (návnady) může trvat několik hodin, přičemž není třeba měnit phishigový server.	Jeden malwarový systém, včetně trojského koně a serveru příjemce, lze vytvořit během několika měsíců. Každá další varianta trvá týden i déle. Když se objeví odpovídající antivirové kódy, přepracování lze provést během několika týdnů až měsíců.

2.3.4. **Pharming**

Jedná se o zdokonaleného, modernějšího a hlavně nebezpečnějšího nástupce phishingu, kdy vlastní odhalení útoku tohoto typu není na straně uživatele tak jednoduché. Nejde o útočení na jednotlivé počítače potažmo uživatele, ale o napadání DNS serveru. Při tomto útoku útočník pomocí upraveného překladu internetových adres na DNS serveru přesměruje všechny uživatele, kteří tento DNS server využívají, na připravené podvodné stránky.

Uživatel se i přes zadání přesné adresy dostane na podvodné stránky umístěné zcela na jiném místě. Většinou se jedná o přesné kopie původních stránek a tak i obezřetný uživatel může být takto oklamán. I v těchto případech jsou tyto útoky prováděny za účelem získání citlivých dat pro jejich následné zneužití. Tyto útoky je možné rozdělit do dvou skupin. Do první skupiny je možné zařadit útoky přímo na DNS server. Jelikož jsou tyto servery páteří internetu je jejich zabezpečení na velmi dobré úrovni a tedy provést změnu překladu internetové adresy bez povšimnutí správce je opravdu velmi obtížné. Proto je zde ještě druhá skupina útoků, ke které se útočníci uchylují. Zde se jedná o útok přímo na konkrétní počítač a to za pomoci jiného škodlivého kódu. Pokud se například podaří útočníkovi nainstalovat do zájmového počítače trojského koně, který na základě dálkového příkazu provede změnu v tzv. hosts souboru má vyhráno. V hosts souboru přepíše IP adresu například internetového bankovnictví na IP adresu svých podvodných stránek a efekt je stejný jako u první skupiny. Potom už pouze záleží na propracovanosti podvodných stránek, jak moc se podobají těm originálním. [13], [14]

2.3.5. **Počítačové pirátství a Warez**

Tento druh trestné činnosti je velmi rozšířen mezi uživateli internetu skrz všechny věkové kategorie. Historie počítačového pirátství a warezu je starší než sama historie internetu. Počátky počítačového pirátství jsou už v nelegálním kopírování audio kazet se softwarem her na osmibitové počítače. Vytváření trhu warezu je relativně pomalé a tedy opravdový boom nastal až s nástupem rychlého internetu. Tuto komunitu tvoří uzavřená skupina lidí, kteří zpřístupňují pirátské kopie na internetu.

2.3.6. **P2P a Cybersquatting**

P2P (Peer to Peer) je označení pro síť kde její označení, tedy rovný s rovným označuje způsob komunikace v síti. Jde o síť kde oproti klasické síti Klient - Server probíhá komunikace přímo mezi klienty a s přibývajícím počtem těchto uživatelů rychlost této sítě roste. P2P síť vlastně pojem server vůbec nezná, jelikož zde vůbec není používán. V dnešní době je tento druh sítě používán především k výměně dat mezi uživateli.

Pojem Cybersquatting není v dnešní době už tak aktuální, jako tomu bylo v minulosti. Jedná se o blokování internetových domén. Zaregistrování domény s názvem firmy, produktu, instituce či jiné zájmové oblasti dával prostor k následným spekulacím. Tento druh činnosti zažíval největší rozmach v době rozšiřování internetu a vstupu velkých firem na tuto síť s prezentací nových výrobků.

2.4. **Zajištění objektů zkoumání**

2.4.1. **Ohledání místa činu**

Ohledání místa činu je mimo jiné i zajištění odpovědí na základní kriminalistické otázky (Co, Kdy, Kde, Kdo, Jak, Čím, Proč). V případě ohledání místa činu u specifických trestných činů, jako jsou trestné činy spojené s počítačovou kriminalitou, je důležité nezanedbat širší místo činu, tedy nejenom místo u konkrétního počítače a samotný počítač, ale provedení kompletní domovní prohlídky v širším okruhu. Zákonnost a podmínky domovní prohlídky jsou uvedeny v trestním řádu a tato práce se jimi nebude podrobně zabývat. Může se jednat jak o skryté datové nosiče, tak o jiný materiál související s danou trestnou činností. Důležitým faktorem u těchto domovních prohlídek je moment překvapení, kdy osoba podezřelá nemá šanci jakýkoli materiál zničit či pozměnit. Na místě činu je třeba postupovat dle platných a osvědčených postupů, aby nedošlo k přehlédnutí či opomenutí důležité skutečnosti. Samozřejmostí je kompletní podrobné zadokumentování jak samotné prohlídky, tak zajišťování jednotlivých důkazů. Jedná se o fotodokumentaci, video dokumentaci, plánky jednotlivých prostor a umístění důkazních prostředků a jejich seznamy. Při zajišťování samotného počítače je nutné v první řadě zajistit možnost odpojení od zdroje, tedy jeho vypnutí a následné převezení na specializované pracoviště k podrobnému zkoumání. Při tom je třeba kompletně zajistit všechny vstupy a výstupy z počítače plombou a opět nesmí chybět podrobné zadokumentování, aby zde byla zabezpečena síla důkazu a nebylo možné udělat jakýkoli zásah do zajištěných dat. U externích nosičů dat je postup obdobný.

2.4.2. **Analýza objektu**

Znalecká zkoumání relevantních skutečností související s událostí trestného činu, které souvisejí přímo či nepřímo s trestným činem, prováděné za účelem získání důkazů použitelných v trestním řízení jsou v kriminalistice nazývány expertizou. Tyto expertizy, jako je forenzní analýza dat, při odhalování a vyšetřování trestné činnosti provádějí specializovaní pracovníci Kriminalistického ústavu Praha. Tyto expertizy pro soukromé subjekty také provádí externí firmy zabývající se touto analýzou. Jelikož i zde může dojít ze strany firmy ke zjištění, že došlo ke spáchání trestného činu, a je tedy třeba zabezpečit důkazní váhu zjištěných skutečností při předání orgánům činným v trestním řízení, jsou stanovena jistá obecná pravidla pro zpracování a dokumentaci. Jedná se o zásady:

- Legality - veškeré informace, předměty, stopy, dokumenty, data apod., která slouží jako vstupní materiály pro forenzní analýzu, musí být získána, pořízena či zhotovena legálním způsobem.
- Integrity - veškerá práce se vstupními daty musí být prováděna tak, aby bylo zcela zřejmé, že nemohlo dojít k úmyslné či neúmyslné změně nebo manipulaci s daty při analýze, jako je například pozměnění kdo, kdy, kde, jak a proč s daty pracoval před touto analýzou.

- Opakovatelnosti / přezkoumatelnosti - jedná se o použití takových metod a zadokumentování daných postupů takovým způsobem, aby bylo možné tou samou nebo ekvivalentní metodou ověřit správnost závěrů, která analýzou vyplynula.
- Nepodjatosti - nezávislost subjektu, který danou analýzu na zájmovém objektu / předmětu provádí.
- Detailní dokumentace - je naprosto neodmyslitelnou součástí forenzní analýzy a to hlavně z důvodu prokazování závěrů, které z forenzní analýzy vyplynuly, tak k prokázání, že nedošlo k porušení žádných výše uvedených zásad.

Aby byly zajištěny jednotlivé zásady, jsou postupy zkoumání v rámci trestního řízení podrobně zadokumentovány od samotného zajištění předmětu až po samotné ukončení analýzy specialistou kriminalistického ústavu Praha. Jakákoli manipulace je podrobně zaznamenána s časem, druhem a postupem manipulace, kdo manipulaci prováděl a s jakým výsledkem. Pokud to okolnosti dovolují je ve většině případů pořizováno i video dokumentace celé manipulace, aby se předešlo spekulacím a zpochybňování důkazní váhy závěrů před soudem. Například při vyhledávání dat na Harddisku je před samotnou analýzou udělán klon tohoto disku a na něm jsou teprve použity metody k získání a vyhledání dat. Obdobně se postupuje se všemi paměťovými medii z důvodu zamezení pozměnění či poškození dat na zájmovém nosiči. [15], [16]

2.4.3. **Znalecký posudek**

Výsledek expertizy je zaznamenán do znaleckého posudku, který představuje vrcholné stádium znaleckého zkoumání. Skládá se ze tří částí.

- Úvod - jsou zde uvedeny údaje o osobě znalce (znalecké instituce), uvedení kdo expertizu nařídil, stručný popis důvodu expertizy, jaké materiály a důkazní prostředky byli předloženy ke zkoumání.
- Nález - zde je znalcem detailně popsán objekt zkoumání, přesný postup, výsledky a použité metody a prostředky použité při analýze. Dále je zde uvedeno, zda došlo k pozměnění, poškození či zničení zkoumaného objektu. U metod uvede znalec důvod použití konkrétních metod použitých v průběhu expertizy. Výsledky a průběh je zadokumentován různými dostupnými metodami dle důkazního významu. U některých výsledků, je-li to potřeba z důvodu vysvětlení vztahové otázky ke zkoumanému objektu, jsou uvedeny i základní vědecká východiska a metody.
- Závěrečná část - obsahuje odpovědi na otázky, které byly znalci zadány, tedy jeho zjištění na základě provedených analýz. Povinnými součástmi písemného znaleckého posudku

jsou dále podpis znalce, razítko znalce a v případě, že je znalec zapsán v seznamu znalců a tlumočníků a vede si znalecký deník, je ještě připojena tzv. znalecká doložka.

Další součástí znaleckého posudku je také dokumentace pořízená znalcem. Ta slouží k detailnějšímu seznámení s postupem, který znalec zvolil, s ukázkou celého průběhu zkoumání i jeho jednotlivých částí, uvádí jednotlivé použité metody a názorně ukazuje závěry a výsledky provedené expertizy. [15]

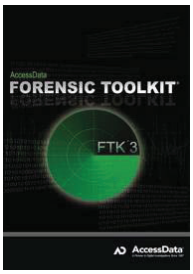
2.5. Nástroje pro forenzní analýzu

Forenzní analýzu dat je možné spustit i v skromnějších podmínkách než je Kriminalistický ústav Praha nebo fundovaná soukromá firma zabývající se touto problematikou. K tomuto účelu jsou na trhu dostupné analyzátory, které lze úspěšně použít i pro soukromé účely k provedení vlastní analýzy.

- EnCase - Nástroj od firmy Guidance Software, Inc. na snadné shromažďování, zpracovávání, analyzování a vytváření forenzních důkazů jak s počítačů tak smartphonů. U verze 7 se dá zakoupit licence za $ 3,495.

Obr. 6 EnCase

- Smart - je volně šiřitelný softwarový nástroj firmy ASR Data pracující na OS Linux, který byl navržen a optimalizován pro podporu odborníků, zabývajících se forenzní analýzou dat a pracovníků informační bezpečnosti. Je volně ke stažení na stránkách firmy.
- Macforensicslab - jedná se o forenzní nástroj splňující náročné podmínky pro vyšetřovatele zabývající se digitální forenzní analýzou. Je konstruován tak, aby plně využil sílu systému Mac OS X. Poslední verze je 4.0, která je dostupná za $1,495 na stránkách firmy.
- PyFlag - nástroj napsaný v Pythonu, určený pro OS Linux. Tento forenzní nástroj není už od roku 2007 dále vyvíjen.
- Forensics Toolkit - je sada produktů, která zahrnuje i nástroje pro mobilní telefon. Umožňuje přihlášení více uživatelů a provést forenzní analýzu dat přes webové rozhraní. Ke své činnosti a urychlení využívá databáze Oracle. Cena tohoto produktu je $2,995.



Obr. 7 Forensic Toolkit

- Hachoir - je framework pro manipulaci s binárními soubory: různé rozpoznávané formáty, extrakce metadat, hledání souborů v každém binárním datovém proudu (forenzní), zobrazení obsahu souboru, apod.
- iLook - komplexní sada počítačových forenzních nástrojů používaných k získání a analýze digitálních medií pro OS Windows.
- Virtuální stroje - nejedná se přímo o forenzní nástroje, ale mohou být využity k následné forenzní analýze jinými nástroji s tím, že spustíme software z HDD na jakémkoli počítači včetně instalovaného OS. Jedním z rodiny těchto softwarových nástrojů používaných k vizualizaci je VMware. Pomocí softwaru, např. Liveview, ProDiscover, vytvoříme z obrazu disku image s konfigurací pro VMware, což nám právě umožňuje i bez původního hardware pracovat s původním systémem a nainstalovaným softwarem.

3. Phishing

3.1. Phishing

Tato metoda používaná pro získávání důvěrných informací od uživatelů se v minulosti postupně rozšířila po celém světě a všude "slavila" úspěchy. I dnes se můžeme s pokusy o získání důvěrných informací tímto způsobem setkat, i když díky zvyšování počítačové gramotnosti uživatelů a jejich současné opatrnosti, to phishers nemají už zdaleka tak jednoduché, jak tomu bylo v minulosti. Pevná definice phishingu není nikde uvedena a jeho forma se neustále vyvíjí. Na základě znalostí lze napsat popis této metody k nelegálnímu získávání důvěrných informací.

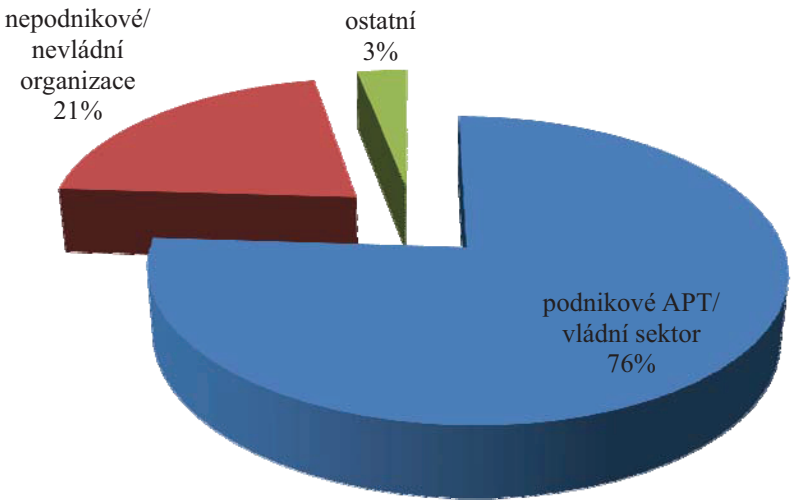
Jedná se tedy o podvodné získávání citlivých dat od uživatelů pomocí rozesílání hromadných e-mailů, které odkazují na fiktivní webové stránky institucí, jako jsou například banky, sociální sítě apod. Tyto stránky jsou vytvořeny jako věrné kopie na podvodných serverech. Rozesílání e-mailů mají většinou na starosti stroje vytvořené přímo phishers k danému účelu, které rozesílají vytvořený e-mail na automaticky generované adresy. Tyto maily vystupují jako instituce, které jsou natolik fundované a známé, aby se dostaly k bankovnímu účtu uživatele, informacím o něm, nebo přístupovým právům. Mají naprosto stejný design, jako používá fingovaná instituce.

Při odhalování phishingu ho můžeme rozdělit do několika skupin podle hlavních identifikačních rysů:

- nástroj pro rozesílání hromadné pošty a jeho vlastnosti
- zvyky v oblasti odesílání pošty jako jsou styly, rozvrhy mailu apod.
- druh systému v počítači používaného pro rozesílání spamu (kde se e-maily vytvářejí)
- druh systému používaného pro umístění phishingového serveru
- struktura phishingového serveru na který je uživatel přesměrován včetně HTML, JS, PHP apod.

První phishingový útok směřovaný na bankovní a finanční instituce byl zaznamenán v červenci 2003. Jeho terčem se staly E-loan, E-gold, Wells Fargo a Citibank.

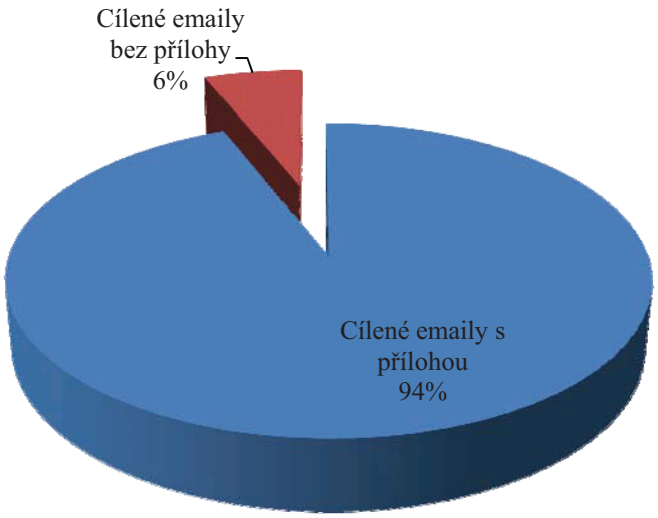
Nebezpečnost v tomto druhu nelegálního získávání osobních a důvěrných dat spočívá v napadení nejslabšího článku v zabezpečení a to je lidský faktor. Je zde k tomu použito sociální inženýrství, a to v tom směru, aby doručený mail uživatele přesvědčil, že odkaz je bezpečný a ten pokračoval na podvodném serveru bez podezření na nějaké podvodné jednání. Zde dochází ke sběru dat a následné uložení k dalšímu využití. [10]



Obr. 8 Podíl cílených útoků na jednotlivé organizace a cíle

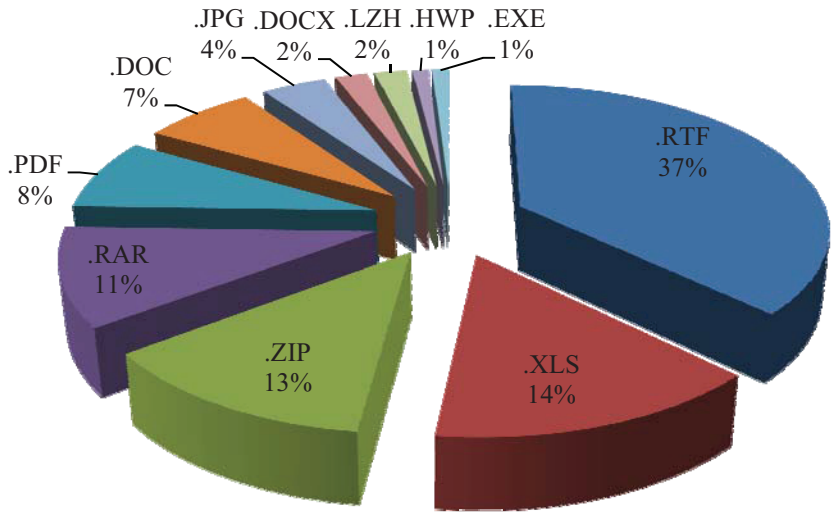
Podle nových výsledků shromážděných společností Trend Micro, který je na špici v oblasti informační bezpečnosti, za období únor až září roku 2012, vytváří celých 91 % cílených útoků e-mail se spear phishingem. Označení spear phishing je používán pro typ phishingu, který v poslední době zaznamenává velký nárůst. Tento typ při útocích využívá informace o cílových objektech, kterými jsou především instituce a vládní organizace (viz. Obr. 8.) o nichž je spousta informací na internetu a jejich webových stránkách. Aktivistické skupiny při své značné aktivitě na sociálních sítích také poskytují při organizování kampaní a snaze rozšířit svou členskou základnu spousty informací. Tímto postupem má následný útok větší pravděpodobnost úspěchu a to z toho důvodu, že je přímo nasměrován na některé osoby a tedy je konkrétnější a osobnější. V těchto emailech není použito obecné oslovení, jak tomu bylo u klasického phishingu, ale může se zde objevit například jméno příjemce, jeho pracovní zařazení či funkce.

Útočníci zde také předpokládají využití známých praktik, které jsou v organizacích běžné a to přeposílání emailů v rámci interní sítě mezi zaměstnanci. Tímto způsobem je možné škodlivý malware rozšířit bez větší námahy a ještě tímto získají na důvěryhodnosti. Tímto způsobem se samozřejmě zvyšuje i předpoklad proniknutí k důvěrným informacím a jejich vlastní získání.



Obr. 9 Rozdělení spear-phishingu dle přítomnosti přílohy v emailu

U spear-phishingu, jsou ve většině případech, k emailu připojeny soubory (viz Obr. 9). Útočníci zejména využívají přípony souborů, které jsou hojně užívány v elektronické komunikaci jako přílohy a tedy mohou spíše působit dojmem přílohy zaslané skutečně důvěryhodným zdrojem. Typy souborů, které jsou využívány k těmto útokům, jsou používány s různou četností (viz. Obr. 10.). [17]



Obr. 10 Využití jednotlivých přípon souborů při spear-phishingu

Ochrana proti tomuto druhu útoků je obdobná jako proti klasickému phishingovému útoku s tím, že zde musí být větší opatrnost a obezřetnost u uživatelů, kteří zde při šíření škodlivého emailu v rámci organizace hrají nezanedbatelnou úlohu.

3.2. Tvorba pharmingových/phishingových stránek

Ať už phishing nebo pharming oba pracují s podvodnými webovými stránkami. Pokud se u phishingu už podaří hromadně rozeslaným emailem přesvědčit některého uživatele, ať klikne na odkaz v něm obsažený, jde o následnou propracovanost podvodných webových stránek. Ty musí do detailu vypadat tak, aby přesvědčili, že se jedná o původní originální stránky instituce, ke které se vztahují data, která chce útočník získat.

Jeden ze softwarů, který se k tomuto účelu dá výborně použít je WinHTTrack Website Copier, aktuálně ve verzi 3.44-4. Tato aplikace je dostupná ve 32bitové a 64bitové verzi pro Windows 2000, XP, Vista a 7 pod názvem WinHTTrack, případně jako přenosná varianta bez instalátoru. Jedná se o aplikaci, která dokáže stáhnout html kód webové stránky na HD počítače včetně všech JavaScriptů. V aplikaci je možnost nastavení do jaké hloubky odkazů chcete kód stáhnout a z toho vyplývá i datová a časová náročnost uložení. Následně nic nebrání tomu, upravit kód stránek tak, aby se zapsaná data uživatelem ukládala do vlastní databáze. Po upravení stránek vybrat vhodný webhosting s adresou, která nápadně připomíná tu původní originální, umístit zde upravené stránky a server spustit. Posledním krokem je hromadné rozeslání důvěryhodného emailu s odkazem na takto vytvořené stránky a pouze čekat kolik lidí se nachytá a údaje na těchto upravených stránkách zadá.

3.3. Detekce phishingu u komerčních nástrojů

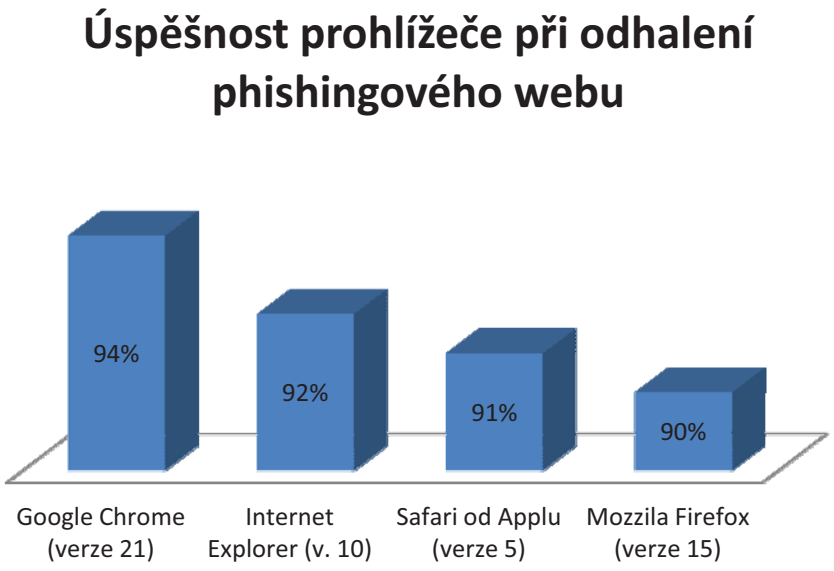
Nástroje na detekci phishingu jsou v dnešní době implementované jak do emailových klientů, tak do internetových prohlížečů. Detekci u těchto nástrojů můžeme prezentovat na dvou produktech. Prvním z nich je Office Outlook od firmy Microsoft a druhý je Google Chrome od firmy Google.

Detekce phishingu u poštovního klienta Outlook je realizován přes filtr Junk E-mail Filter, který je možné si stáhnou na webu Office Online. Poštovní klient následně prochází jednu zprávu po druhé, a pokud ji Junk E-mail Filtr nepovažuje za spam, ale zjistí ve zprávě podezřelé odkazy, odešle ji do Junk E-mail složky. Každá taková zpráva je v této složce převedena do formátu prostého textu a všechny odkazy, které zpráva obsahuje, jsou vypnuty. Pokud dojde k tomu, že Junk E-mail Filtr považuje zprávu za podezřelou, nebo spam, ale odesílatel, nebo doména jsou na seznamu bezpečných odesílatelů, pak zpráva zůstane ve složce Doručená pošta, ale všechny odkazy jsou opět zakázány. [19]

Bezpečné prohlížení prostřednictvím Google Chrome chrání uživatele před phishingem a malwarem dvěma způsoby. Do prohlížeče se nejdříve stáhne seznam informací o stránkách, které mohou obsahovat škodlivý software nebo být zneužívány k phishingu. Pokud se adresa URL navštívených webových stránek shoduje s některou adresou ze seznamu, kontaktuje

prohlížeč servery Google, aby pro rozhodnutí získal více informací. Pokud počítač na základě zjištěných informací následně rozhodne, že se jedná o rizikové stránky, může zobrazit varování na tyto stránky. Bezpečné prohlížení také napomáhá chránit uživatele před cílenými phishingovými útoky (spear phishing) i v případě, kdy společnost Google stránku ještě nezná a tedy ještě nebyla zařazena na seznam phishingových stránek. Google Chrome proto analyzuje obsah navštívených stránek a pokud zde vznikne podezření na možný phishing uživatele upozorní. [18]

Prohlížeče chrání uživatele před phishingem různými formami, které můžou mít mnoho úrovní. Nejjednodušší ochrana proti podvodným stránkám využívaných při phishingu je použití tzv. černé listiny, kde jsou uvedeny všechny známé podvodné weby a jsou provozovateli těchto seznamů pravidelně aktualizovány. V říjnu 2012 provedli výzkumníci z NSS Labs test prohlížečů, kde každých 6 hodin po dobu 10 dnů zkoušeli schopnost prohlížečů rozeznat phishingový web. Vzorky byly do testu neustále přidávány. V tomto testu nejlépe obstál Google Chrome (v. 21) který měl úspěšné odhalení, tedy zablokování v přístupu v 94% phishingových webů. Ostatní prohlížeče, které byly do testu zahrnuty, si vedly obdobně a dosáhly minimálně 90% úspěšnosti (viz. Obr. 11).



Obr. 11 Výsledky testu prohlížečů v odhalování podvodných webů uvedené v procentech

Další z možných střípků bezpečnostní skládačky je užívání namísto klasického HTTP užití HTTPS. Zde je komunikace mezi klientem a serverem šifrována a chráněna před datovým odposlechem. Samozřejmě se jedná jenom o ukazatel, který ovšem nemusí být stoprocentní, jelikož si může i phisher zaregistrovat doménu prvního stupně a spustit si ji na zabezpečeném serveru s protokolem HTTPS.

4. Analýza zadání

4.1. Stanovení cíle práce

Cílem této práce je vytvořit nástroj pro detekci phishingu v rámci komunikace prostřednictvím elektronické pošty v oblasti bankovnictví. Jedná se tedy o nástroj, který má uživatele upozornit, pokud doručený email obsahuje odkaz na podvodný web vytvořený za účelem získání důvěrných informací od uživatele ve spojení s bankovnictvím. V tomto směru se jedná vesměs o informace týkající se internetového bankovnictví.

4.2. Návrh metody detekce phishingu spojeného s bankovnictvím

Je všeobecně známo, že banka nikdy nepožaduje po uživateli přihlašovací údaje jako je jméno a heslo zadávat jinam než při přihlašování přímo do internet banky. Lze tedy předpokládat, že se útočník pokusí emailem přesvědčit uživatele, že je třeba se přihlásit do internet banky přes odkaz uvedený v jeho emailu. Jako důvod může uvést cokoli, co bude působit reálně.

Detekce takového emailu může být složitější, než se může na první pohled zdát. Máme známou URL adresu internetového bankovnictví, tedy můžeme pouze porovnat, zda email tento odkaz obsahuje. Tuto doménu I. stupně spolu s protokolem HTTPS, který je vždy použit, srovnáme s odkazem a pokud bude výsledek kladný, jedná se pravděpodobně o zprávu z banky a můžeme předpokládat, že se lze přes tento odkaz bezpečně přihlásit. V tuto chvíli nebudeme brát možnost Pharmingu (přepsání DNS serveru). Problém je v tom, že každý jiný mail bude detekován jako potencionální hrozba. Jak tedy tento problém odstranit?

Jedna z možností je určení klíčových slov spojených s internetovým bankovnictvím a jednotlivými bankami. Tyto by se jako první vyhledali ve zprávě. Pokud by je obsahovala, byla by následně prověřena přítomnost odkazu na internetové bankovnictví. Jestliže by i zde nastala shoda, jedná s největší pravděpodobností o zprávu z banky. Jakmile by však byl detekován odkaz v textu zprávy bez shody s URL internetového bankovnictví, s největší pravděpodobností by se jednalo o odkaz na podvodný web.

Při detekci provedené tímto způsobem je možné rozdělení klíčových slov do kategorií, které by určovali stupeň nebezpečí, že zpráva obsahuje odkaz s podvodnými webovými stránkami.

Další možností detekce by mohlo být vygenerovat různé modifikace domén I. stupně, které budou nápadně podobné té originální a porovnávat je. Jakmile by nastala shoda s jinou URL než tou, která náleží internetovému bankovnictví, byla by zpráva vyhodnocena jako phishing.

Tato možnost je velmi náročná na obsahovou část a není zde zaručeno, že by byly vygenerovány všechny možnosti. Proto nebyla zvolena tato metoda, ale metoda první.

4.3. Nástroje a prostředky použité při realizaci

Celá aplikace je realizována pomocí nástroje Microsoft Visual Studio 2010 od firmy Microsoft Corporation. Toto vývojové prostředí může být použito pro vývoj konzolových aplikací a aplikací s grafickým rozhraním, tak i pro vývoj aplikací Windows Forms. Pro řešení a realizaci zadání byl zvolen poslední uvedený druh aplikace tj. Windows Forms.

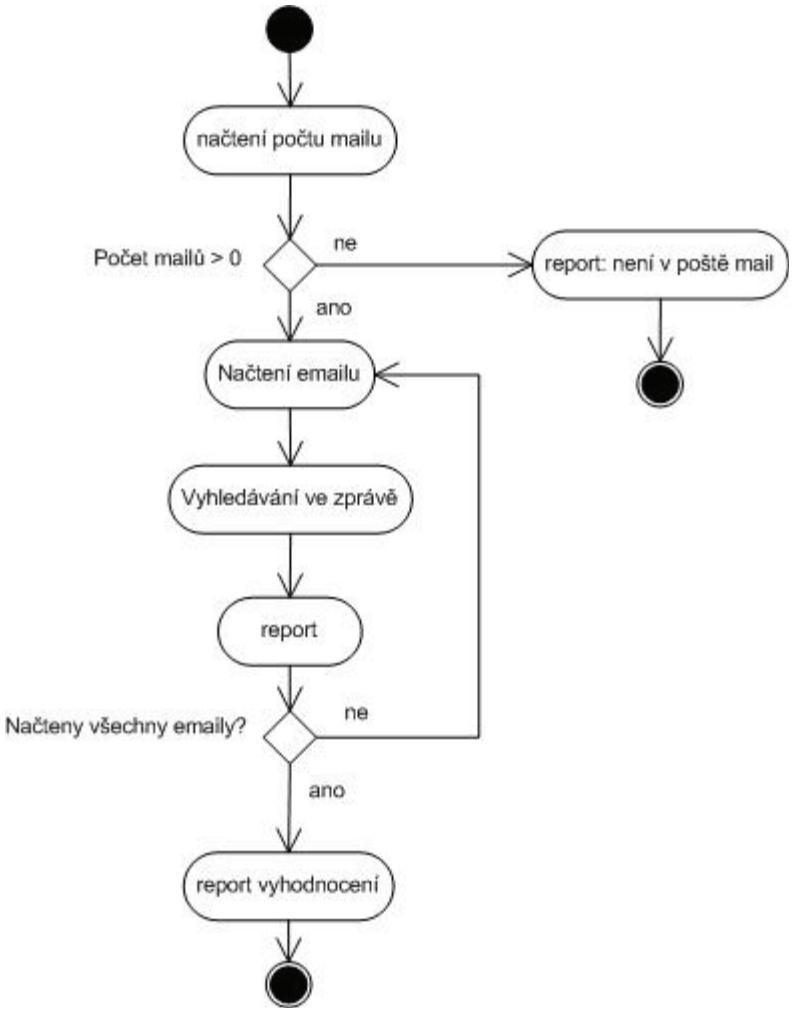
Jako programovací jazyk byl dle zadání zvolen C# (C sharp). V tomto jazyce je naprogramovaná celá aplikace s využitím XML.

4.4. Popis řešení (aplikace)

V první řadě je vytvořen poštovní klient určený ke stahování elektronické pošty pomocí protokolu POP3. Přihlášení k účtu je možné pouze výběrem ze seznamu emailových adres, které jsou uloženy spolu s kompletními přihlašovacími údaji v XML souboru. Pro zajištění určité bezpečnosti přístupových hesel jsou tato před uložením do XML kódována. Po úspěšném přihlášení je možné spustit automatické prohlížení. Tato volba každou zprávu po stažení projde a vyhledá klíčová slova a odkazy.

Mezi volby aplikace patří možnost uložení posledního nastavení při spuštění kontroly zpráv pro případ následného automatického spuštění, jehož nastavení je k dispozici ve volbách. Toto ukládání potažmo načítání nastavení je realizováno XML souborem. V aplikaci bude řešeno nastavení všech variant defaultně jako DISABLE. Uživatel bude muset po prvním spuštění jednotlivé požadované funkce v menu zapnout. Pokud zvolí uložení po ukončení a načtení po spuštění, zůstane jeho volby přednastaveny. Další volby nastavení kromě těchto dvou bude možnost spuštění jako minimalizované na liště, automatické prohlídnutí po spuštění, automatické vyhledání všech bankovní serverů (Obr. 12) a jako poslední bude možnost nastavení zpoždění spuštění aplikace.

Aplikace bude možno spouštět automaticky se zpožděním, minimalizovanou na liště, kdy tato aplikace projde všechny emaily na přednastaveném účtu a každý zvlášť vyhodnotí v report listu. Tento bude při normálním zobrazení aplikace v okně vedle okna s textem emailu. Jako celkový report bude okno s počtem jednotlivých hrozeb rozdělených do 3 kategorii - vysoká hrozba, střední hrozba, nízká hrozba. Jednotlivé kategorie budou voleny podle obsahu klíčových slov ve zprávě. Tyto klíčová slova budou stejně jako URL adresy jednotlivých bank uloženy v XML souboru a budou aplikací načítány vždy po spuštění.

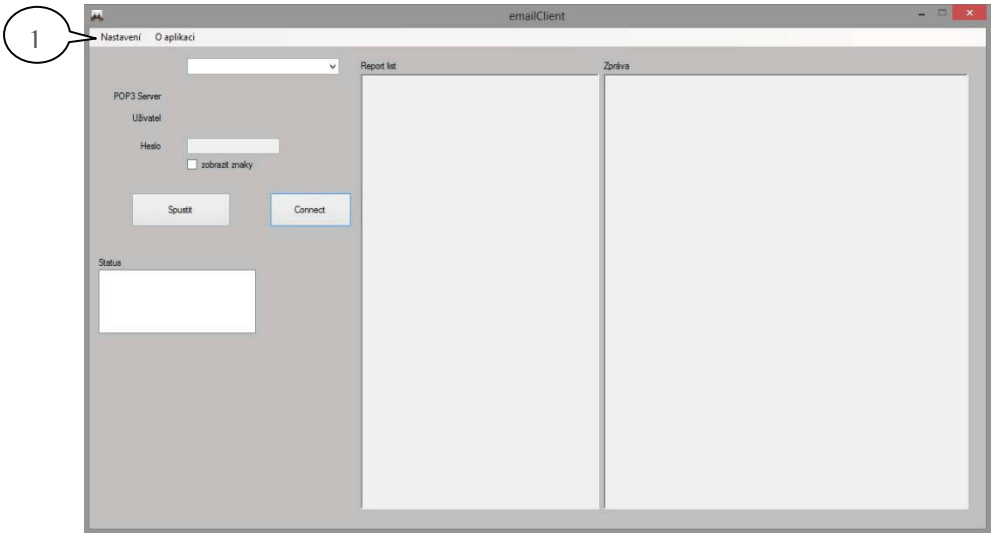


Obr. 12 UML diagram automatického načtení emailů a vyhledávání ve zprávách

5. Implementace

5.1. Analýza

Implementaci jsem vytvořil ve vývojovém prostředí Visual Studio 2010 programovacím jazykem C#. Základem je aplikace, která stahuje z poštovního serveru emaily pomocí protokolu pop3.

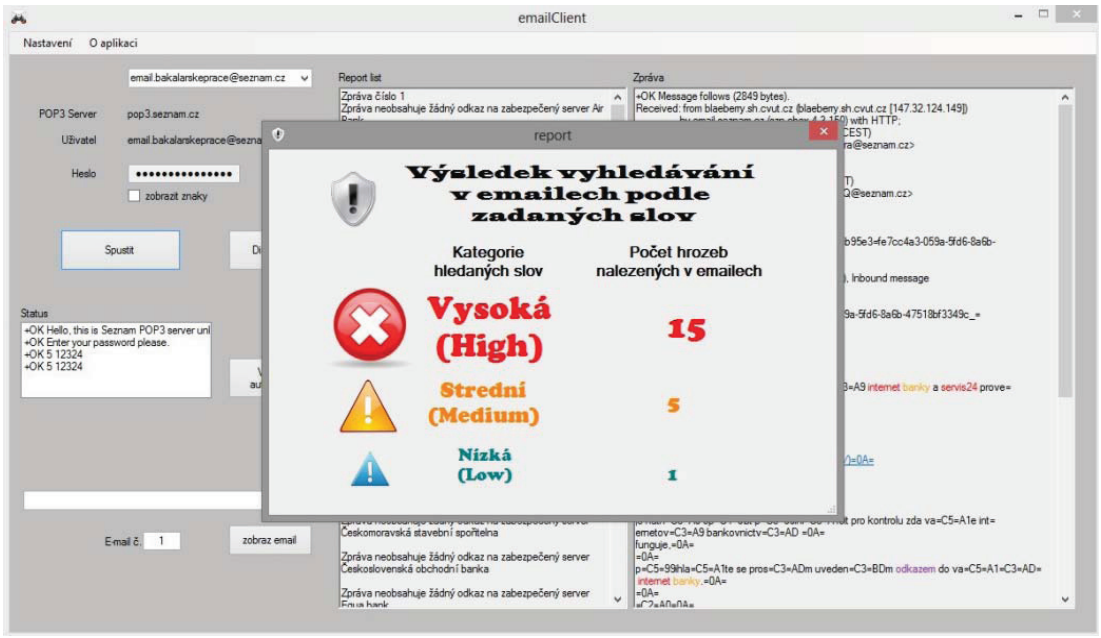


Obr. 13 Aplikaci je po prvním spuštění potřeba nastavit (1)

Postupné řešení jednotlivých částí projektu jsem řešil z důrazem na funkčnost a jednoduchost. Jako základní princip jsem zvolil detekci oficiálních adres URL internetového bankovnictví a následně klíčových slov uložených v XML souboru. Tato slova by měla být volena individuálně dle jednotlivých bankovních institucí. Aby u aplikace byla zaručena určitá flexibilita, vytvořil jsem v nastavení možnost editovat jednotlivé záznamy souborů XML. Použil jsem zde tři XML soubory, které zajišťují data, jež jsou důležitá pro funkčnost aplikace. Jedná se o soubory pro ukládání a editaci uživatelských účtů (*users.xml*), bankovních institucí (*banks.xml*) a uživatelského nastavení aplikace (*setting.xml*). Klíčová slova nástroje, která jsou určena pro bližší identifikaci potencionální hrozby v jednotlivých emailech, jsou také uložena v *banks.xml* jako další elementy jednotlivých bankovních institucí, s atributy nastavenými dle závažnosti hrozby při přítomností těchto slov v emailu.

Pro usnadnění použití, jsem oproti vytvořené původní verzi, kde si uživatel banku, jejíž internetové bankovnictví chtěl detekovat, volil sám, rozšířil o možnost automatického procházení jednotlivých emailů s kompletním vyhledáváním. Jde o postupné načítání emailů a jejich následná kontrola na přítomnost odkazů jednotlivých bankovních serverů a přiřazených klíčových slov. Tuto operaci jsem z důvodu přehlednosti, kromě uvedení

výsledků v *report listu* ukončil zobrazením okna „report“, s celkovým počtem nalezených klíčových slov, rozdělených dle vážnosti potencionální hrozby. (Obr.14)



Obr. 14 Výsledný report aplikace po automatickém spuštění

Po spuštění aplikace se při inicializaci načte také soubor *setting.xml*, kde je uložena předvolba možností nastavení. Pro první spuštění jsem hodnoty přednastavil, nebo je ponechal prázdné. Z tohoto důvodu je dobré si nejdříve aplikaci po spuštění pomocí nastavení přizpůsobit. (Obr.13)

```
<?xml version="1.0" encoding="utf-8" ?>
<nastaveni>
  <nacteni>True</nacteni>
  <ulozeni>False</ulozeni>
  <zobrazeni>False</zobrazeni>
  <start>False</start>
  <zpozdeni>False</zpozdeni>
  <upozorneni>True</upozorneni>
  <sekund>0</sekund>
  <jmeno></jmeno>
  <heslo></heslo>
  <protokol></protokol>
  <nazev></nazev>
  <adresa></adresa>
</nastaveni>
```

nastavení aplikace

emailový účet

banka

Přihlášení k emailovému účtu je realizováno z ComboBoxu, do kterého jsou jednotlivé emailové účty načteny ze souboru *users.xml*. V tomto souboru jsou uloženy všechny potřebné údaje k přihlášení. Po výběru jsou automaticky vyplněny potřebné údaje.

```
<?xml version='1.0' encoding='utf-8'?>
<users>
  <user name="">
```

```
    <jmeno></jmeno>
    <heslo></heslo>
    <protokol></protokol>
  </user>
</users>
```

Samotná hesla k účtům jsem před uložením do XML souboru z důvodu určitého zabezpečení zašifroval pomocí metody FromBase64String.

```
//kódovaní hesla
//Rozloží text na bajty
byte[] bajty = Encoding.Unicode.GetBytes(textBox1.Text);
// Převede je na zašifrovaný řetězec pomocí base64
passKod = Convert.ToBase64String(bajty);
```

Zakódované heslo je uloženo u zkušebního emailového účtu v users.xml

```
<?xml version="1.0" encoding="utf-8"?>
<users>
  <user name="email.bakalarskeprace@seznam.cz">
    <jmeno>email.bakalarskeprace@seznam.cz</jmeno>
    <heslo>YgBhAGsAYQBsAGEAcgBzAGsAYQBwAHIAYQBjAGUA</heslo>
    <protokol>pop3.seznam.cz</protokol>
  </user>
</users>
```

Po přihlášení je úspěšnost potvrzena v okně Status, kde je v případě úspěšného přihlášení i počet mailů na serveru a jejich celková velikost v bajtech.

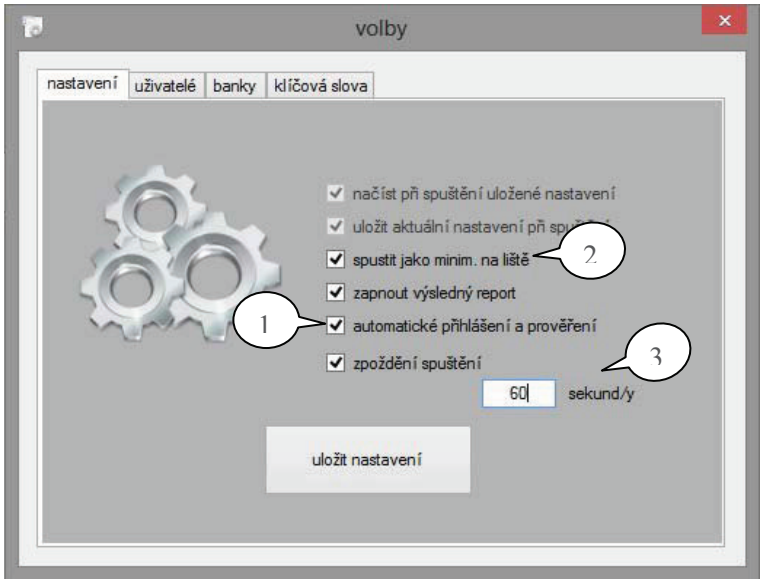
Při našem spouštění aplikace jsem samozřejmě přednastavil zkušební emailový účet, který je jinak nutné zadat přes ***Nastavení → uživatelé.***

Banky a jejich internetové adresy jsou uloženy v *banks.xml*. Klíčová slova je možné sice navzájem mezi bankami kopírovat, ale to nepovažuji za zcela vhodné z důvodu specifikace jednotlivých internetových bankovnictví a klíčových slov, která mohou přispět k odhalení eventuální hrozby.

```
<banka naz="Česká spořitelna">
    <nazev>Česká spořitelna</nazev>
    <adresa>https://www.servis24.cz/</adresa>
    <slova>
      <slovo kat="High" text="www.serviis24.cz"/>
      <slovo kat="High" text="servis24"/>
      <slovo kat="High" text="internet"/>
      <slovo kat="High" text="banka"/>
      <slovo kat="Medium" text="banky"/>
      <slovo kat="Low" text="odkazem"/>
      <slovo kat="Low" text="www.csas.cz/banka"/>
    </slova>
  </banka>
```

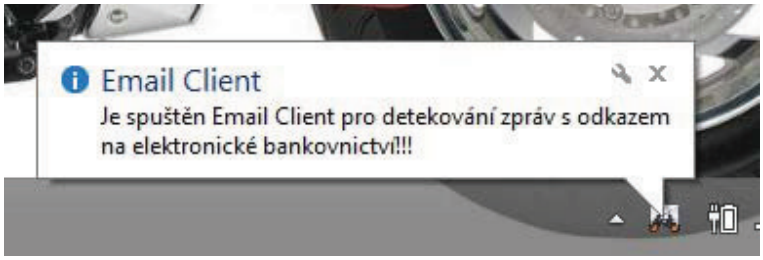
Pokud jsou všechny výše uvedené podmínky splněny a všechna data jsou zadána, lze s aplikací dále pracovat.

Jednotlivá tlačítka jsem navolil tak, aby byla uživatelsky přijatelná a ovládání bylo intuitivní.



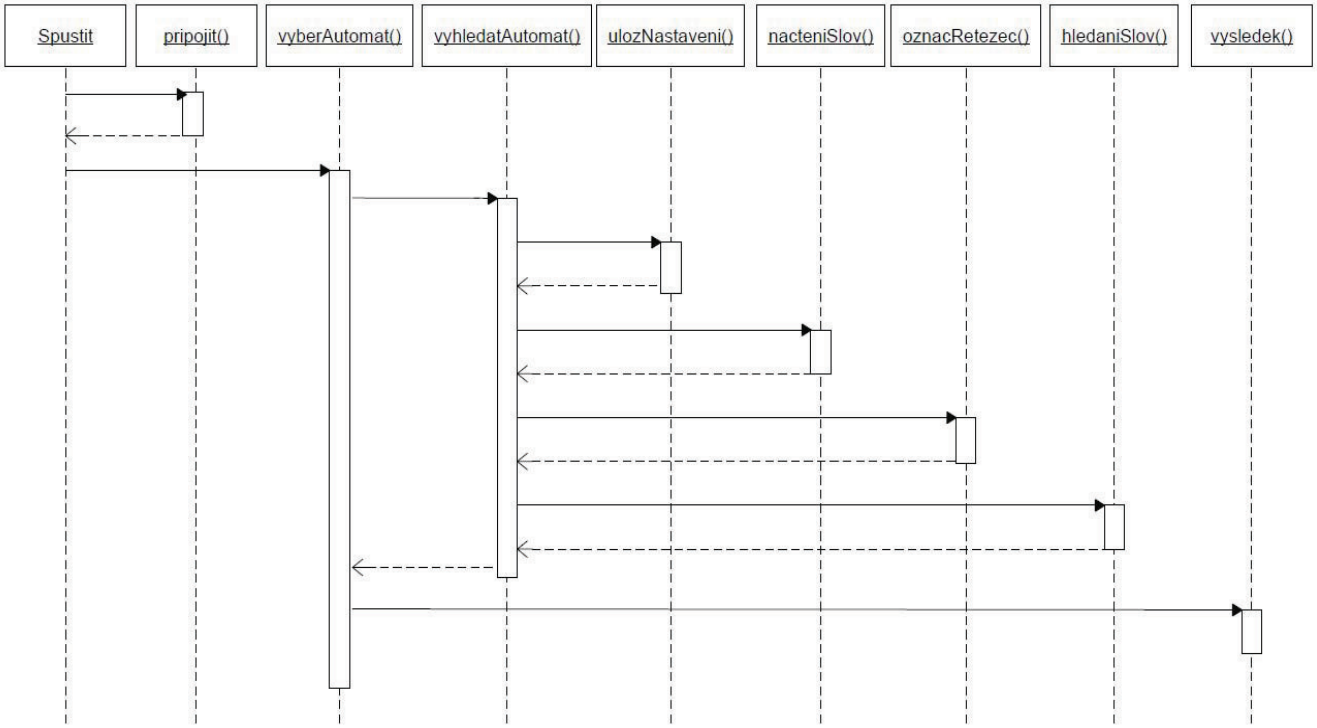
Obr. 15 Nastavení aplikace pro případné spuštění při startu operačního systému, kde je možné nastavit také automatické prověření zpráv (1), minimalizované zobrazení (2) a zpoždění při spuštění aplikace (3)

Jak jsem výše uvedl, pro větší pohodlí uživatele jsem v aplikaci vytvořil možnost nastavení režimu úplného automatického spuštění spolu s kompletním prohlédnutím emailů. Takto nastavenou aplikaci lze zařadit mezi programy spouštěné při startu operačního systému. Pro tuto alternativu jsem vytvořil další volitelné možnosti a to zpožděného spuštění a spuštění v minimalizované podobě na liště. (Obr. 15) V případě zvolení těchto možností minimalizovaná aplikace po nastaveném čase začne automaticky stahovat a kontrolovat zprávy z poštovního serveru. Možnost nastavení časové prodlevy jsem zde vytvořil z důvodu vyčkání na kompletní naběhnutí systému a všech programů před spuštěním kontroly zpráv. Aplikace v tomto případě na své spuštění upozorní zobrazením hlášení o spuštění (Obr. 16) a o ukončení kontroly zpráv informuje zobrazením okna "report", jak je uvedeno v následujícím textu.



Obr. 16 Zobrazené hlášení při spuštění aplikace v minimalizovaném stavu

Postupné volání funkcí v tomto režimu spuštění je znázorněno na sekvenčním diagramu. (Obr. 17)



Obr. 17 Sekvenční diagram automatického režimu aplikace

V rámci úspěšného přihlášení jsem ze zpráv *STAT* (konkrétně posledního řádku) tedy komunikace mezi klientem a serverem, zjistil počet emailů ve schránce.

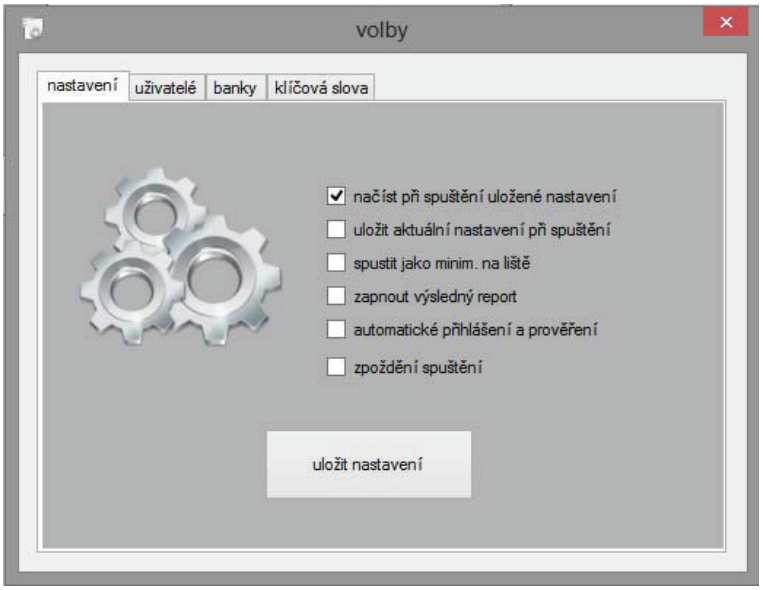
```
// získání počtu e-mailů z řetězce STAT
string[] vstup = posledni_radek.Split(' ');
string vystup = vstup[1];
pocet_mailu = Convert.ToInt32(vystup);
```

Pokud tedy proběhne přihlášení úspěšně, a je zjištěn počet zpráv ve schránce, může být zavolána funkce *vyberAutomat()*. Zde jsem pomocí cyklu *for* postupně načetl všechny zprávy. Po každém dokončeném načtení zprávy je volána další funkce *vyhledatAutomat()*. Tato funkce prohlídne načtenou zprávu, zda neobsahuje některý z odkazů na bankovní server, vypíše do *report listu* výsledek hledání a zavolá další funkce:

- *ulozNastaveni()* - zavolá funkci, která pokud je tato volba nastavena, uloží hodnoty do setting.xml pro eventuelní příští spuštění.
- *nacteniSlov()* - jde o funkci, která naplní jednorozměrná pole podle kategorie klíčovými slovy.
- *oznacRetezec()* - pokud je řetězec ve zprávě nalezen, tato funkce označí barevně jeho výskyt ve zprávě.

- *hledaniSlov()* - funkce, která prohledává text zprávy a označuje barevně nalezená klíčová slova. Jednotlivé barvy jsou rozděleny podle potencionálního rizika.

V tento okamžik je ukončena funkce *vyhledatAutomat()* a je zavolána funkce *vysledek()*. Zde se jedná pouze o zobrazení nového okna s celkovým reportem s celkovým počtem nalezených klíčových slov.

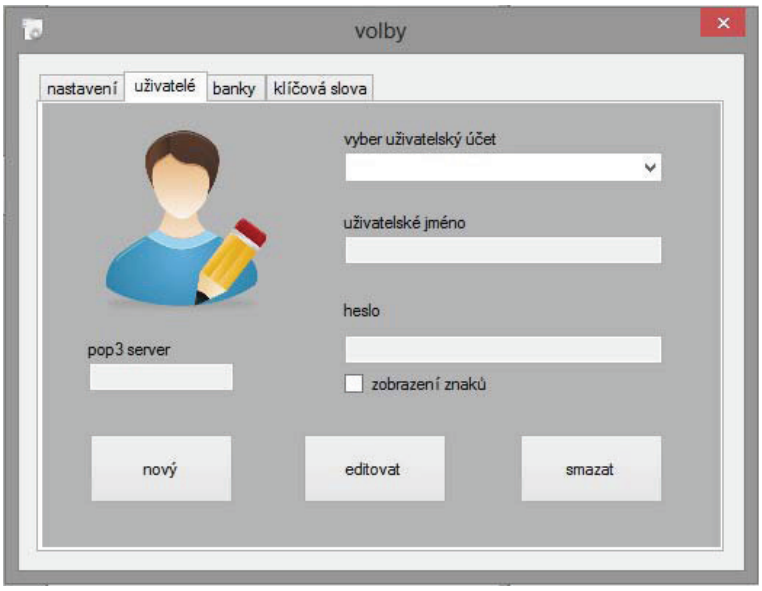


Obr. 18 Okno nastavení aplikace

U aplikace jsem vytvořil volby, kde uživatel může nastavit více možností spouštění, zobrazování a načítání. Tyto se nastavují v horním menu "**nastavení**". Myslím si, že jsem zvolil přehlednou formu, která vznikla sjednocením jednotlivých položek menu a to

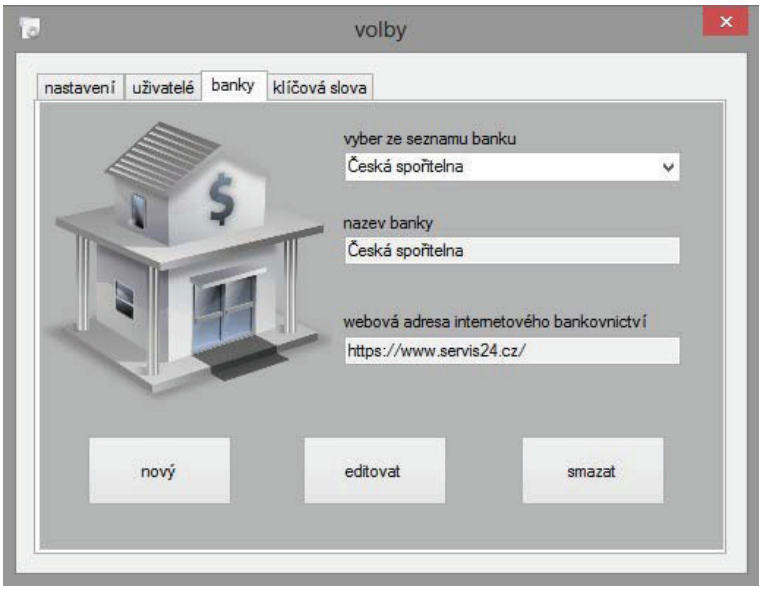
- nastavení – možnost změnit podmínky při spuštění, zobrazení, ukládání, načítání (Obr. 18),
- uživatelé – spravování přihlašovacích údajů k emailovým účtům (Obr. 19),
- banky – umožňuje editovat banky a jejich adresy internetového bankovnictví (Obr. 20)
- klíčová slova – vkládání nebo mazání klíčových slov u jednotlivých bankovních institucí (Obr. 23)

Ve většině případů jsem v této aplikaci deklaroval proměnné jako globální. Tento způsob jsem zvolil především proto, že lze tyto proměnné jednoduše předávat včetně jejich hodnot mezi funkcemi.



Obr. 19 Okno na spravování uživatelských účtů

Postupným vývojem a přidáváním dalších funkcí potřebných pro správný chod aplikace se stal kód relativně mohutný. V některých případech by samozřejmě bylo možné funkce sjednotit a tím snížit vlastní mohutnost kódu, ale myslím, že by to bylo spíše na škodu. Při samotném spuštění aplikace nemá členění a mohutnost kódu žádný citelný vliv na jeho běh ani výsledky, a proto si myslím, že toto členění může mít své výhody při úpravách, nebo rozšiřování některých částí aplikace.



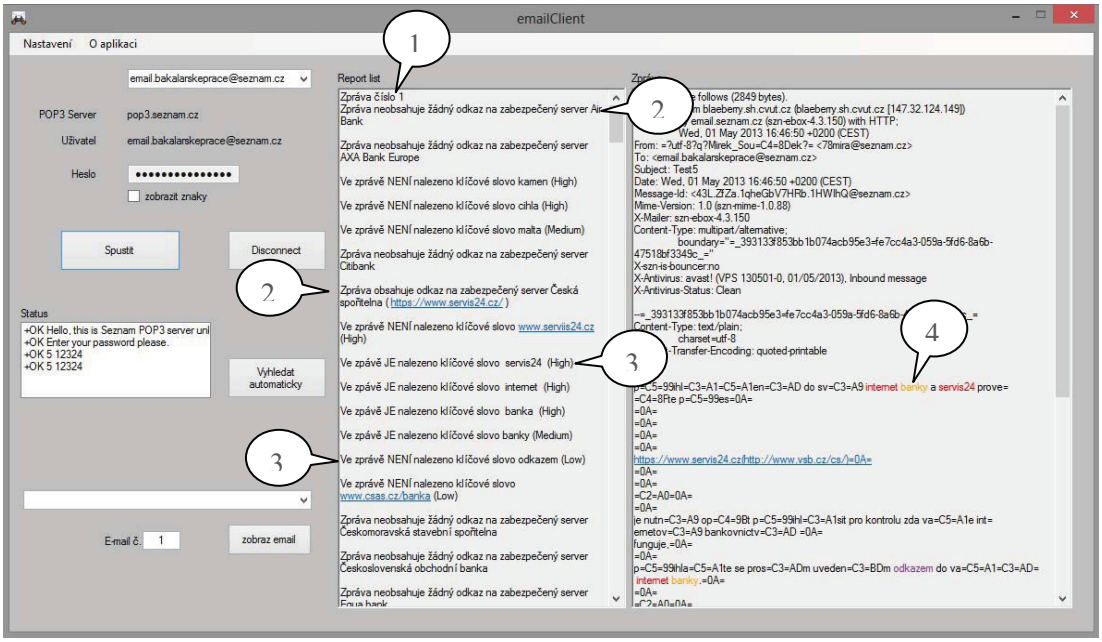
Obr. 20 Okno na spravování bankovních institucí a webových adres jejich internetového bankovnictví

5.2. Testování

Vlastní testování jsem napoprvé provedl na několika svých emailových účtech. Zde bylo testování bez problémů. Samotná detekce klíčových slov proběhla na těchto účtech dle očekávání v naprostém pořádku a nebyla nalezena potencionální hrozba.

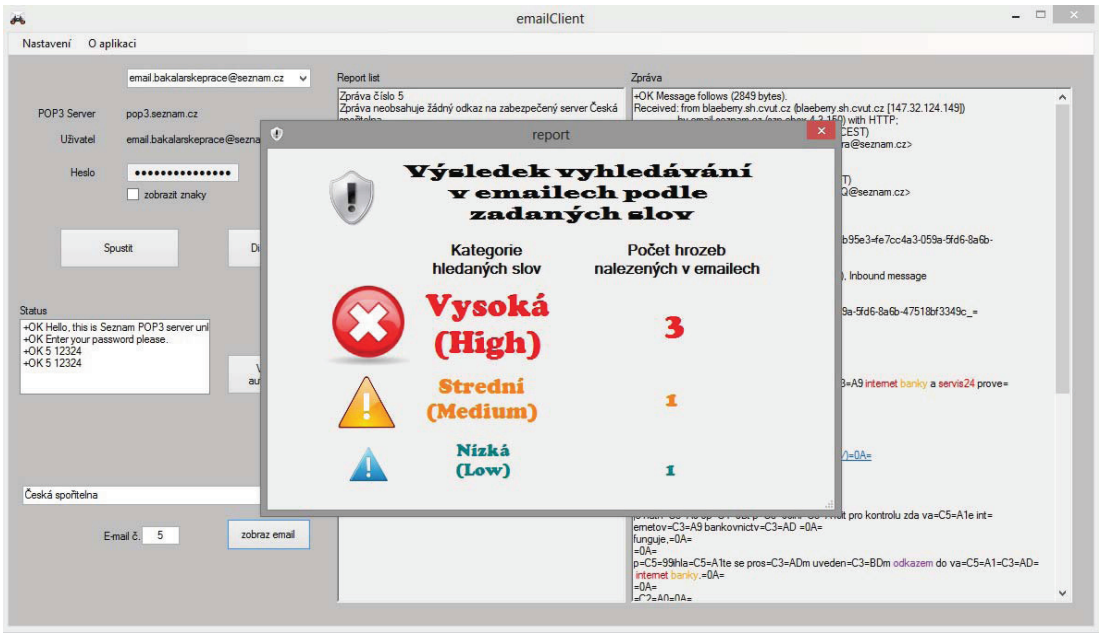
Jelikož toto testování na mých účtech probíhalo bez přítomnosti zpráv, které by obsahovali potencionální hrozbu, vytvořil jsem emailový účet *email.bakalarskeprace@seznam.cz* na který jsem umístil několik zpráv, které by v normálním případě mohly být danou hrozbou.

Po nastavení automatického spouštění a následného prověření všech emailů na tomto novém účtu byl výsledek tohoto prověření viz.Obr.14. Po zavření okna "report" jsou v okně "report list" vidět výsledky vyhledávání jednotlivých webových adres a klíčových slov.(Obr.21)



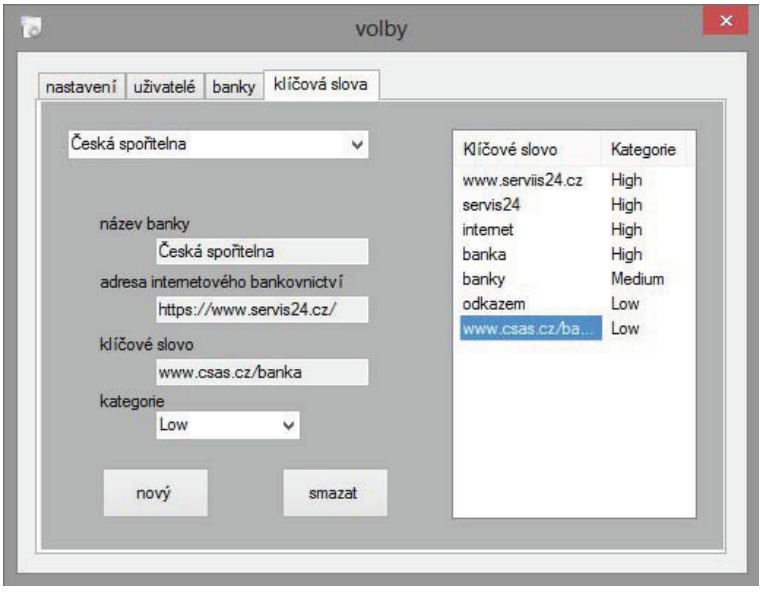
Obr. 21 Výsledný přehled po automatickém vyhledávání: 1- číslo zprávy, která byla prohlížena, 2- report zda zpráva obsahuje oficiální odkaz na internet banku, 3- report zda zpráva obsahuje klíčové slovo, 4- barevné odlišení nalezených klíčových slov

Pokud nástroj nalezne email, ve kterém je odkaz na bankovní server, nebo některá klíčová slova, a chceme si ho prohlédnout, je možné si ho pomocí tlačítka **zobraz email** znovu načíst a prověřit na přítomnost odkazu směřujícího na určitý bankovní server a klíčová slova. (Obr. 22)

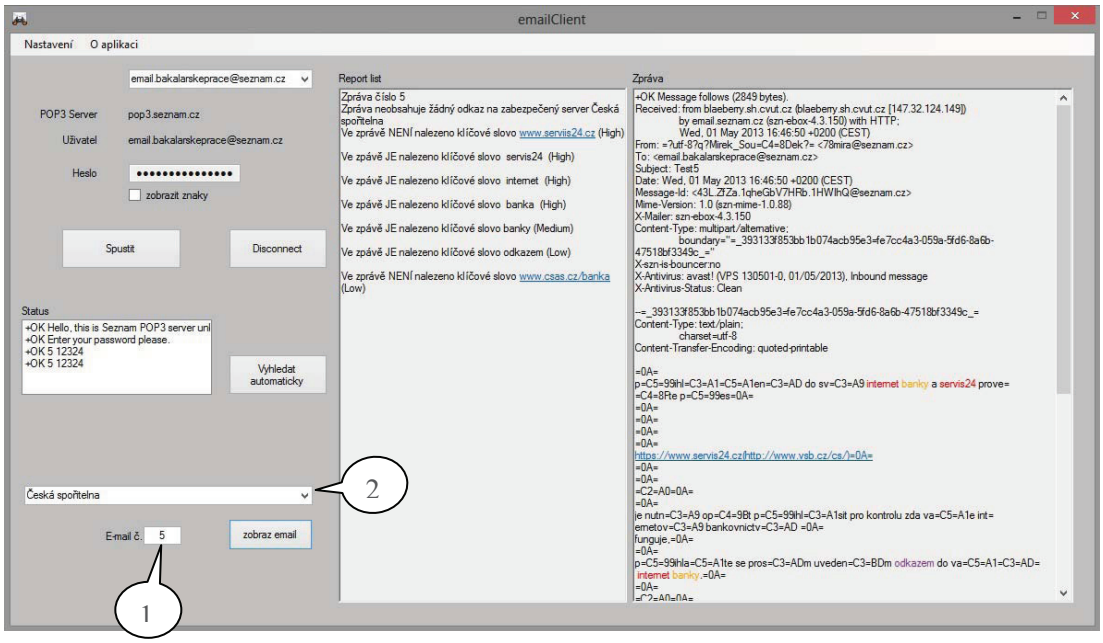


Obr. 22 Výsledný přehled po vyhledávání konkrétního bankovního serveru s klíčovými slovy v nastaveném emailu

Opět po zavření okna "report" můžeme vidět detailní výsledky vyhledávání odkazu na bankovní server vybrané banky spolu s výskytem zadaných klíčových slov (Obr. 23) v dané zprávě. (Obr. 24)



Obr. 23 Ukázka zadaných klíčových slov patřících k bance Česká spořitelna přes volby v nastavení aplikace



Obr. 24 Detailní report vyhledávání ve zprávě číslo 5 (1), kde jsme hledali bankovní server a klíčová slova náležící k České spořitelně (2)

Průběh celého testování proběhl v naprostém pořádku. U prvního testování, tedy soukromého emailového účtu, byla delší doba při načítání zpráv ze serveru, což bylo zapříčiněno větším celkovým objemem dat obsažených na emailovém účtu. Výsledky týkající se detekce potencionální hrozby byli však i přes toto uspokojivé.

Následné testování u speciálně vytvořeného účtu pro tyto účely, kde byly umístěny zprávy z potencionální hrozbou (odkaz na bankovní server, výzva k přihlášení apod.), proběhlo taktéž bez komplikací.

Celkové výsledky testování ukázaly, že zvolený způsob řešení, tedy pomocí vyhledávání řetězců v elektronické poště, je dostačující k odhalení potencionální hrozby. Kvalita a spolehlivost je dána pouze výběrem klíčových slov.

6. Zhodnocení

Výsledky testování spolu s analýzou zadání dávají dohromady celkový obraz aplikace pro detekci phishingu v elektronické poště v oblasti bankovnictví. Nástroj přímo zaměřený na bankovní komunikaci v rámci emailu je aplikace, kterou nelze brát za zcela dostačující a nelze se tedy spolehnout pouze na tento druh ochrany. Tato aplikace dle výsledků testování na vytvořeném emailovém účtu, kam byli zaslány různé druhy potencionálních phishingových emailů, je v odhalování tohoto druhu počítačové kriminality relativně úspěšná, avšak musíme připustit, že se jednalo o maily známých způsobů útoků a klíčová slova byla volena přesně podle těchto kriterií. Nelze tedy vyloučit při dnešním tempu dalšího vývoje kvality těchto útoků případné selhání, tedy neodhalení zprávy, která bude mít znaky phishingu. V našem případě se takové selhání neprojevilo, což můžeme přičíst znalosti problematiky a vědomí tohoto nebezpečí.

V této aplikaci by bylo určitě možné některé části kódu efektivně rozšířit, pokud bychom na ni nehleděli jako na úzkoprofilovou utilitu a tím by se zvýšila možnost jejího využití při práci s elektronickou poštou. Lze s ní ovšem pracovat i v této verzi v širším záběru a to velmi jednoduše. Aplikace stahuje z poštovního serveru poštu, zprávu po zprávě a vyhledává řetězce zadané v banks.xml. Na tyto potom upozorňuje jak v okně aplikace tak celkovým reportem. Je tedy jednoduché přepsat tento XML soubor přes menu aplikace a následně nám vyhledá vše dle našeho přání.

7. Závěr

Cílem této práce bylo vytvoření nástroje pro detekci phishingu v rámci komunikace prostřednictvím elektronické pošty se zaměřením na komunikaci v oblasti bankovnictví. Pro bližší pochopení této problematiky jsme v předchozích kapitolách absolvovali stručné seznámení s problematikou počítačové kriminality. Byly zde nastíněny druhy útoků, se kterými se může uživatel v dnešní době setkat i způsob zajišťovaní stop při ohledání místa činu v případě spáchání trestného činu.

Samotný nástroj byl naprogramován za pomoci Microsoft Visual Studio 2010 v programovacím jazyku C# (Sharp).

Na základě zjištěných skutečností týkajících se phishingu a po nastudování již odhalených útoků na bankovní komunikaci z historie byla pro navrhovaný nástroj zvolena metoda detekování odkazů oficiálních webových stránek jednotlivých bankovních institucí spolu s vybranými klíčovými slovy, které jsou obsaženy v textu zprávy. Aplikace tedy přímo nedetekuje phishing jako takový, ale na základě zvolených parametrů, upozorňuje na potencionální rizikové emaily. Toho je zde docíleno vhodným zvolením klíčových slov ve spojení s oficiálními webovými adresami internetového bankovnictví.

V dnešním nepřeberném množství veškerého zabezpečovacího softwaru, aplikací a utilit je aplikace navržená v této práci spíše určitým druhem "majáku", který má upozornit na možné riziko, než klasickým zabezpečovacím nástrojem. Může usnadnit práci při kontrole emailu tím, že upozorní na potencionální hrozbu phishingu a může tedy i nepřímo zabránit úniku citlivých údajů, rozhodně ale stoprocentně neochrání uživatele před vlastní neopatrností.

Jak bylo výše uvedeno, v bankovním sektoru tento druh útoků není už tolik obvyklý a běžný, ale i přesto věřím, že tato aplikace má jisté opodstatnění. Nikdy by se člověk neměl vzdát ostražitosti a opatrnosti co se týče osobních a důvěrných informací. Zadávání osobních údajů při různých registracích na internetových stránkách s příslibem výhry, nebo jiné výhody je rozšířenou formou sběru dat. Právě proto by si každý uživatel měl uvědomit, že před zadáním jakýchkoli osobních dat je dobré vědět, komu je poskytuje a přesvědčit se, že informace, které zadává, jsou opravdu nezbytné a nutné, a že například stránky náleží opravdu té organizaci nebo instituci, za jejichž stránky je uživatel považuje. Pokud si člověk opravdu není jistý, je určitě lepší než bezhlavě zadat údaje a pak hořce litovat, ověřit si stránky nebo email telefonicky. Pokud člověk zadá jméno nebo telefonní číslo a následně je obtěžován reklamními hovory, je to nepříjemné, ale nic ho to nestojí, kdežto odcizení přihlašovacích údajů, ať už je to k sociální síti nebo internetovému bankovnictví, ohrožuje přímo identitu člověka, jeho pověst a jeho majetek.

Zdroje

[1] Česká Republika. Zákon číslo 40/2009 Sb., Zákon trestní zákoník. In: Sbírka zákonů 2009, (citace 24. 11. 2012). Dostupné na: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw= zakon&what=Cislo_zakona_smlouvy

[2] HARRIS, S., HARPER, A., EAGLE, C., NESS, J., LESTER, M. *Gray Hat Hacking: The Ethical Hacker's Handbook* [*Hacking - manuál hackera*]. Translated from the Czech by ZNAMENÁČEK T. 1. vyd. Praha: Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5

[3] U.S.DEPARTMENT OF JUSTICE (Federal Bureau of Investigation, Laboratory Division). *Handbook of Forensic Services.* Revised 2007. An FBI Laboratory Publication Federal Bureau of Investigation. Quantico, Virginia. 197 s. ISBN 978-0-16-079376-9

[4] MUSIL, S. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů.* 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2000. 281 s. ISBN 80-86008-80-0

[5] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vydání. Praha: Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2

[6] Council of Europe. *Convention on Cybercrime*. Budapest, November 2001. [cit. 20. 12. 2012]. Available on: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[7] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách*. Soudní inženýrství [online]. 2006, 5, č.1 [cit. 20. 12. 2012]. 21 s.
Dostupné na: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

[8] RISK ANALYSIS CONSULTANTS, s. r. o. *Forenzní zkoumání digitálních důkazů - příručka pro vyšetřovatele*: metodický materiál pro vyšetřovatele, kteří se při své práci setkávají se zkoumáním digitálních důkazů [online]. Verze 1.02. [cit. 20.12. 2012]. 40 s.
Dostupné na: http://www.qualysguard.sk/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328/$FILE/Guide%20051230.pdf

[9] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení*. POLICISTA - měsíčník Ministerstva vnitra [online]. 1998, č. 3 [cit. 20. 12. 2012]. Dostupné na: http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSM-Digit_%C3%A1ln%C3%AD%20forenzn%C3%AD%20anal%C3%BDza-01-2010.pdf

[10] LANCE, J. *Phishing Exposed* [*Phishing bez záhad*]. Translated from the Czech by MOUDRÝ L. 1.vyd. Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1766-1

[11] MICROSOFT. *Spyware, nejčastější dotazy* [online]. 2012. [cit. 20. 12. 2012]. Dostupné na: http://windows.microsoft.com/cs-cz/windows-vista/spyware-frequently-asked-questions

[12] MACICH, J. *Malware: viry, červy a další havěť*. Počítač pro každého [online]. 2008, č. 18 [20. 12. 2012]. Dostupné na: http://ppk.chip.cz/cs/archiv-vydani/r2008/c18-2008/ppk-18-2008-pdf/_files/ppk-18-2008-malware-38-40.pdf

[13] BITTO, O. *Rhybaření střídá pharming.* In: Lupa.cz [online]. 2005. [cit. 20. 12. 2012]. Dostupné na: http://www.lupa.cz/clanky/rhybareni-strida-pharming/

[14] BEDNÁŘ, V. *Pharming je zpět a silnější.* In: Lupa.cz [online]. 2007. [cit. 20. 12. 2012]. Dostupné na: http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/

[15] STRAUS, J. *Kriminalistická taktika*. 2. vyd. Plzeň: Aleš Čeněk, 2008. 291 s. ISBN 978-80-7380-095-6

[16] SVETLÍK, M. *Digitální forenzní analýza a bezpečnost informací*. In: rac.cz [online]. 2010. [cit. 10. 2. 2013]. Dostupné na: http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSM-Digit%C3%A1ln%C3%AD%20forenzn%C3%AD%20anal%C3%BDza-01-2010.pdf

[17] TREND MICRO (EMEA) Ltd. - Central & South Eastern Europe. *Spear-Phishing Email: Most Favored APT Attack Bait.* In: trendmicro.com [online]. 2012. [cit. 6.3.2013].

Dostupné na: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

[18] GOOGLE. *Detekce phishingu a malwaru*. In: support.google.com [online]. 2013. [cit. 10. 2. 3. 2013].Dostupné na: http://support.google.com/chrome/bin/answer.py?hl=cs&answer=99020

[19] MICROSOFT Corporation. *Block or unblock links in suspicious phishing messages*. [Blokování nebo odblokování odkazů v podezřelých phishingových zprávách]. In: office.microsoft.com [online]. 2013. [cit. 10. 2. 2013]. Available on: http://office.microsoft.com/en-us/outlook-help/block-or-unblock-links-in-suspicious-phishing-messages-HA001184193.aspx#BM1

[20] MACICH, J. Moderní prohlížeče vs. phishingové weby. In: Root.cz [online]. 2013. [cit. 24. 4. 2013]. Dostupné na: http://www.root.cz/clanky/moderni-prohlizece-vs-phishingove-weby/

[21] JANGL, M. *Počítačová kriminalita* - diplomová práce. Brno: Masarykova univerzita, Fakulta právnická, 2007. 75 s. Vedoucí diplomové práce Marek Fryšták.