Spamové zprávy a možnost jejich detekce v globální síti Internet

Spam messages and the possibility of their detection in the global Internet

Michal Dvořák

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal DVOŘÁK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Spamové zprávy a možnosti jejich detekce v globální síti Internet**

Zásady pro vypracování:

1. **Uveďte nejpoužívanější metody pro vytváření spamových zpráv.**
2. **Definujte metody využívané pro šíření spamů.**
3. **Srovnejte metodiku a výkonnost jednotlivých bezpečnostních produktů proti šíření spamů.**
4. **Navrhněte řešení ochrany proti spamu pro LAN síť do 5000 klientských PC.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Adámek, Martin: Spam : jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu. Praha : Grada, 2009**
2. **Polčák, Radim: Právo na internetu : spam a odpovědnost ISP. Brno : Computer Press, 2007**
3. **R. Peša. E-mail, spam a greylisting MU. Zpravodaj ÚVT MU, 2007**
4. **Spam , internetový zdroj**
5. **Spam z pohledu zákona , internetový zdroj**

Vedoucí bakalářské práce: **Ing. David Malaník**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtech Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá velmi rozšířenou problematikou poslední doby. Jde o tzv. nevyžádanou poštu neboli spam, která velmi zaplňuje naši emailovou schránku. Zaměřuji se na druhy spamu, nejpoužívanější metody pro vytváření spamových zpráv a metody využívané pro šíření spamových zpráv. Nejen prostřednictvím elektronické pošty, která běží na protokolu SMTP, ale i jiných jako jsou komunikační programy (např. ICQ, QIP a Instant Messaging). V praktické části se budu zabývat srovnáním jednotlivých bezpečnostních SW produktů proti šíření spamu. Navrhnu zabezpečení firemní sítě a ochranu proti spamu.

Klíčová slova: Spam, email, SMTP, ICQ, QIP, SW, síť

ABSTRACT

This work deals with a widespread issue last time. This is the so-called spam or spam that fills our very inbox. It focuses on the types of spam, most methods for the creation of spam and the methods used to spread spam. Not only via electronic mail, which runs on the SMTP protocol, as well as other programs such as communication (such as ICQ, QIP and Instant Messaging). In the practical part, I will deal with comparing different security software products against the spread of spam. A proposal for corporate network security and spam protection.

Keywords:Spam,email,SMTP,ICQ,QIP,SW,network

Na tomto místě bych rád poděkoval vedoucímu práce, Ing. Davidu Malaníkovi za ochotu ujmout se práce, cenných konzultačních hodin a odbornou pomoc při zpracování této bakalářské práce.

Dále bych chtěl poděkovat své rodině za podporu, poskytnuté zázemí a možnost studia na této škole.

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 – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Moje práce bude pojednávat o jednom z nejvíce diskutabilních témat našeho internetového věku. Jde právě o nevyžádanou poštu neboli spam, který denně obtěžuje miliony uživatelů na celém světě. Definovat spam není nijak jednoduché, protože si každý člověk pod spamem může představit úplně něco jiného. Nějaké rozumné vysvětlení je nám nabídnuto na internetovém portálu Wikipedie. „Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem.“ [1]

Ano nejčastějším zástupcem ve spamu je reklama. Setkáváme se s reklamními nabídkami z nejrůznějších oblastí, orientací a služeb. V poslední době se začíná velmi rozšiřovat nabídka finančních služeb. O pornografii již asi není takový zájem jako dříve. Spammeři se už neorientují jen na naše emailové schránky, ale spamy začínají často pronikat i do dalších komunikačních prostředků. Jako jsou např. komunikační programy typu ICQ, QIP či Instant Messaging, nebo také diskusních fór, chatů apod.

Ve své práci rozeberu, jaké jsou typy nevyžádané pošty, a uvedu jejich příklady. Zaměřím se na metody, které jsou využity pro šíření spamu a důkladně je rozeberu. Chtěl bych zdůraznit, že reklama je sice nejčastějším zástupcem, ale vůbec ne tím nejnebezpečnějším. V nevyžádané poště nám hrozí mnohem větší nebezpečí. Spam totiž může přenášet i nebezpečné viry nebo phisingové zprávy, které ochromují náš počítač. Dokonce pomocí takových virů nebo phishingu se spammeři mohou dostat k našim citlivým a osobním údajům nebo k našim heslům do internetového bankovnictví. Dále náš počítač mohou zneužít k distribuovanému rozesílání spamů. Seznámím vás s nejčastějšími způsoby získávání adres pro spammery. Popíšu, jak se má běžný uživatel na internetu chovat, aby zbytečně nevystavoval svou emailovou adresu a tak ulehčoval práci spammerům a jejich robotům. Lidé velmi často nevědomky uvádí své adresy a tím velmi ulehčují práci spammerům.

Jak se vlastně bránit před takovou hromadnou nevyžádanou korespondencí? Na tuto otázku se pokusím zodpovědět v jedné ze svých kapitol. Myslím si, že sto procentní ochrana nikdy existovat nebude, protože by se hlavně musel upravit náš zákon. Určitě se ale dá chránit před spamem na hodně vysoké úrovni, za použití speciálně vytvořených programů, metod a filtrů. Hlavní díl na naší ochraně má ale prevence, kterou podrobně vysvětlím.

Otestuji několik antispamových programů, abych zjistil jak se bránit proti nevyžádané poště v praxi. K testování si vyberu takové programy, které se budou hlavně lišit tím, jestli

jsou poskytovány zdarma nebo se za ně platí. Chci zjistit, na jaké úrovni nás dokážou chránit freewarové programy. Porovnám, zda jsou lepší placené verze nebo freewarové verze antispamových programů. Ve firemních sítích spam může způsobit nemalé škody, tak navrhnu jak se bránit.

Cílem mé práce bude objasnění všech okolnosti kolem spamingu. Proč je ve světě vůbec tolik nevyžádané pošty, proč to lidé vůbec dělají apod. Vysvětlím jak se chovat na internetu a hlavně jak se bránit před spamem. V praktické části otestuji placené a neplacené verze antispamových programů a napíšu svoje doporučení a zkušenosti. Nakonec navrhnu zabezpečení firemní sítě před nevyžádanou poštou.

I. TEORETICKÁ ČÁST

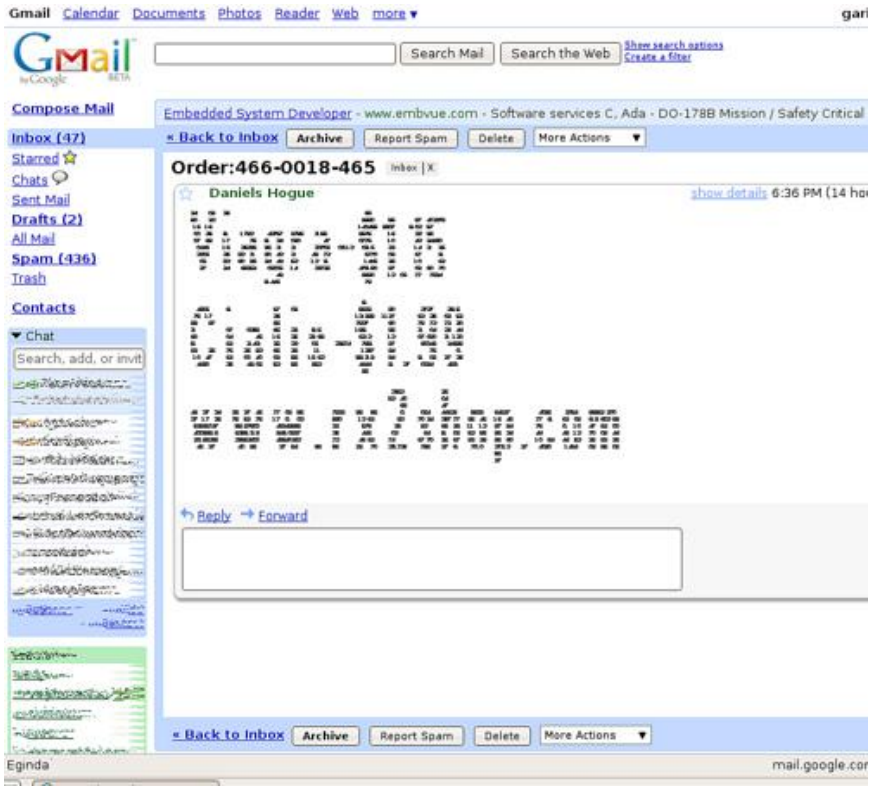
1 METODY PRO VYTVÁŘENÍ SPAMOVÝCH ZPRÁV

Tuto kapitolu bych rozdělil na pár základních bodů. Tyto metody se rozlišují v obtížnosti jejich odhalení. Spammeři vymýšlí a přicházejí s nejrůznějšími metodami, novinkami a posouvají se stále dál a dál. Spamy mají nejrůznější obtížnosti odhalení od relativně snadno odhalitelných až po ty co skoro odhalit nejdou. Řekl bych, že se nikdy nepodaří sto procentně odhalit všechny spamy na našich počítačích.

1.1 Textový spam

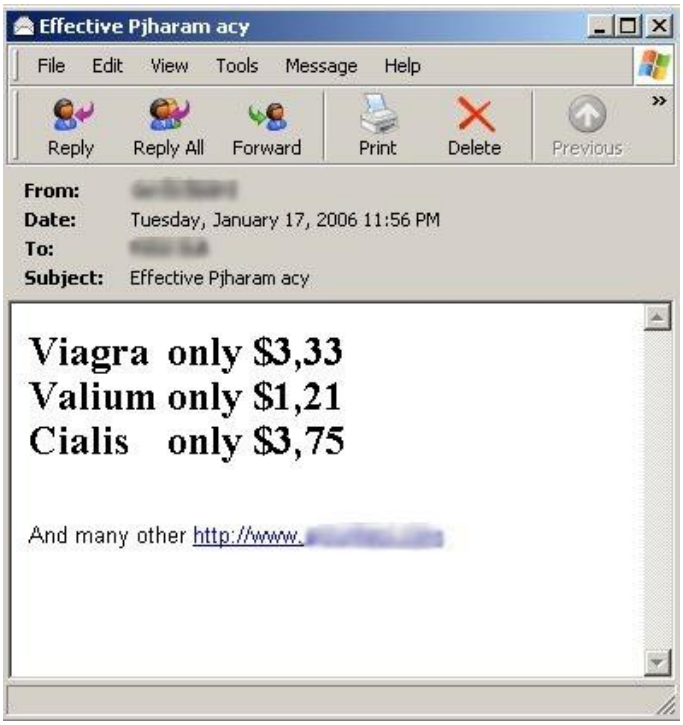
Textový spam je základní metoda, která je podle mě nejrozšířenější a nejvíce distribuovaná. Spammeři hromadně rozesílají textové emaily, které obsahují nejrůznější reklamy, odkazy, viry atd. Na tyto spamy existuje řada antispamových programů a mnoho nejrůznějších filtrů. Dá se říct, že bojovat proti textovým spamům je dnes už mnohem snadnější než kdykoliv dříve. Kombinace filtrů s antispamovými programy nám zaručí určitou bezpečnost. Ale taky záleží na nás uživatelích, jak se budeme na internetu chovat. Tzn. nevystavovat svou emailovou adresu, kde se jen dá. Boj pro nás bude mnohem jednodušší.

Uvedu příklad textové spamu na Viagru, kde se spammeři snaží obejít antispamové filtry jako je např. bayesovský filtr. Kdyby slovo Viagra bylo napsané normálně, tak filtry jej zachytí a nepropustí. Spammeři se to snaží obejít, tak že slovo Viagra složí za pomocí nejrůznějších znaků. Toto je jeden z mnoha příkladů jak se spammeři obcházejí antispamové filtry. Více se tomuto budu věnovat v jedné z dalších kapitol.



Obrázek 1: Textový spam [2]

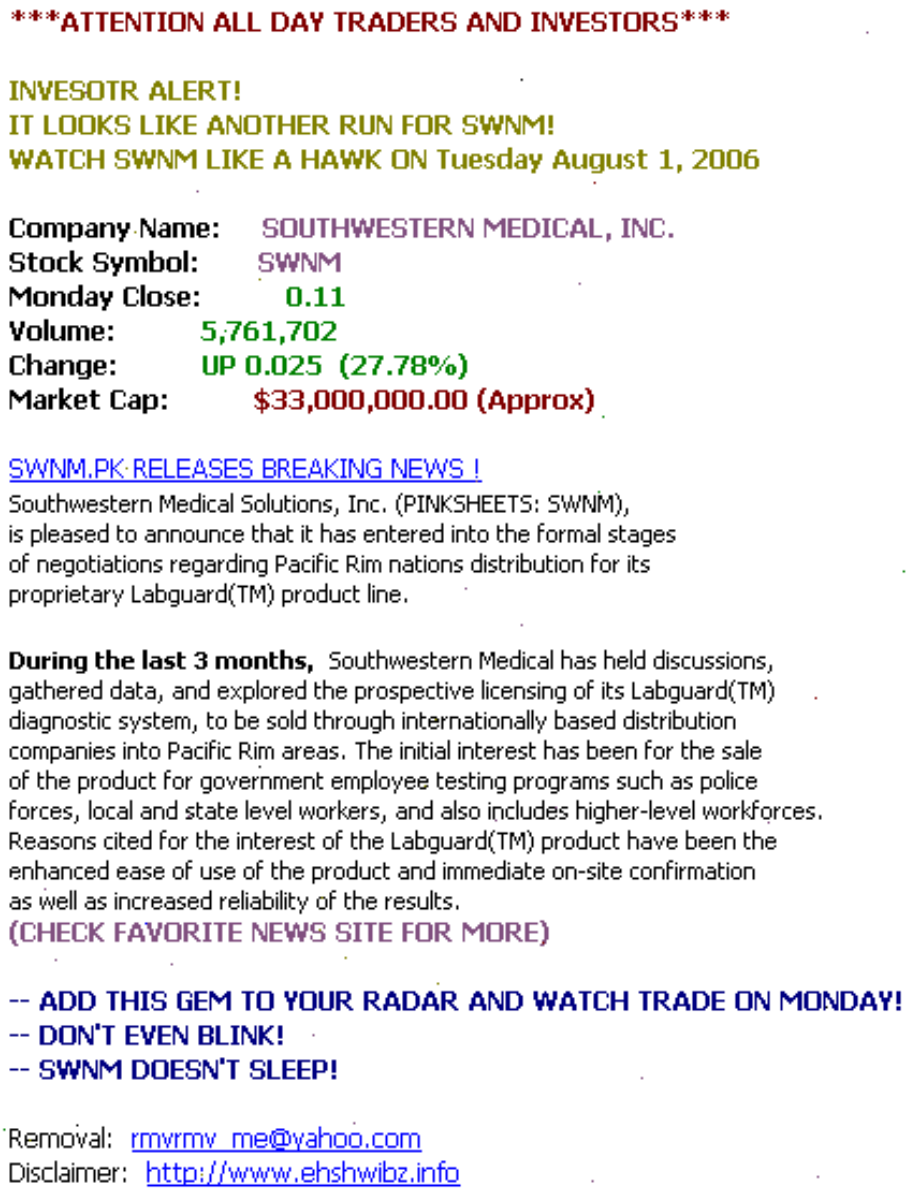
Ještě bych uvedl příklad textového spamu také na Viagru, který by měli filtry bez problémů zachytit.



Obrázek 2: Textový spam na Viagru [3]

1.2 Obrázkový spam

Boj proti virům začíná připomínat boj, proti neustavičným pisatelům virů. Jsou vždycky o krok napřed a klasické metody ochran už pomalu nestíhají stačit. Hitem poslední doby se začínají stávat obrázkové spamy. Je to jeden z dalších problémů, který čím dál tím víc začíná obtěžovat běžné uživatele. Tato metoda rozesílání nevyžádané pošty není v dnešní době ničím novým. Spammeři tuto techniku začali používat více jak před deseti lety. Za poslední dva roky vzrostl zejména objem obrázkového spamu. Podle posledních analýz je tohoto druhu více jak 30% nevyžádané pošty. K obcházení filtrů textu využívá tato metoda grafické podoby.


ATTENTION ALL DAY TRADERS AND INVESTORS

INVESOTR ALERT!
IT LOOKS LIKE ANOTHER RUN FOR SWNM!
WATCH SWNM LIKE A HAWK ON Tuesday August 1, 2006

Company Name: SOUTHWESTERN MEDICAL, INC.
Stock Symbol: SWNM
Monday Close: 0.11
Volume: 5,761,702
Change: UP 0.025 (27.78%)
Market Cap: $33,000,000.00 (Approx)

SWNM.PK RELEASES BREAKING NEWS !
Southwestern Medical Solutions, Inc. (PINKSHEETS: SWNM), is pleased to announce that it has entered into the formal stages of negotiations regarding Pacific Rim nations distribution for its proprietary Labguard(TM) product line.

During the last 3 months, Southwestern Medical has held discussions, gathered data, and explored the prospective licensing of its Labguard(TM) diagnostic system, to be sold through internationally based distribution companies into Pacific Rim areas. The initial interest has been for the sale of the product for government employee testing programs such as police forces, local and state level workers, and also includes higher-level workforces. Reasons cited for the interest of the Labguard(TM) product have been the enhanced ease of use of the product and immediate on-site confirmation as well as increased reliability of the results.
(CHECK FAVORITE NEWS SITE FOR MORE)

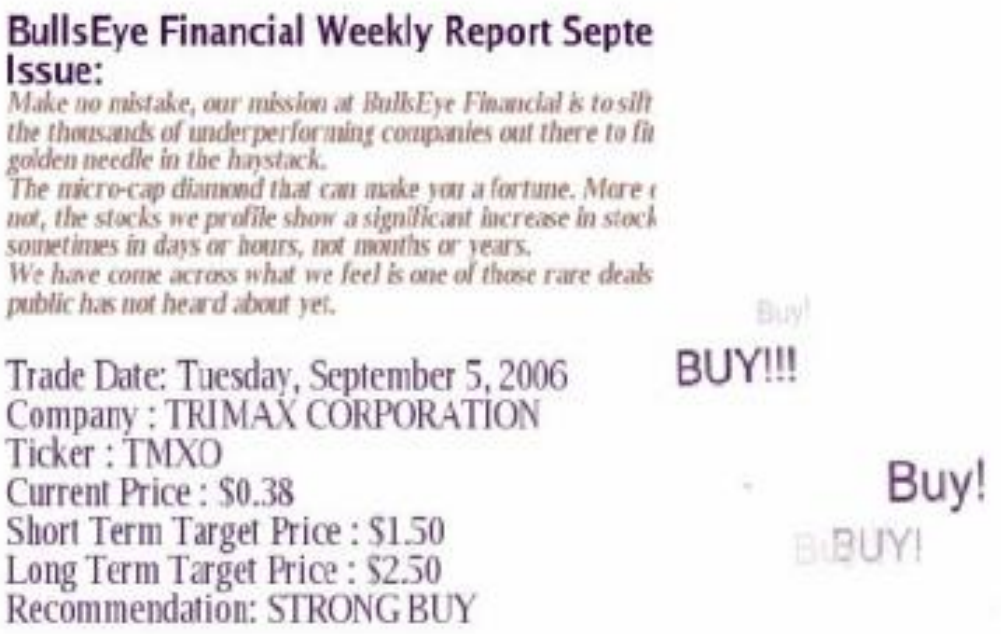
-- ADD THIS GEM TO YOUR RADAR AND WATCH TRADE ON MONDAY!
-- DON'T EVEN BLINK!
-- SWNM DOESN'T SLEEP!

Removal: rmvrmv_me@yahoo.com
Disclaimer: http://www.ehshwibz.info

Obrázek 3: Obrázkový spam [4]

První obrázkové spamy byli relativně snadno detekovány, protože spammeři rozesílaly pokaždé stejný obrázek. Časem si tak antispamové filtry dokázaly vytvořit svou vlastní databázi otisků obrázkového spamu a byli celkem snadné tyto spamy blokovat. Ale v poslední době propracovanost těchto spamů dosáhla značné dokonalost. Dnes se používají obrázky vytvořené tak, aby se nedali strojově číst. Cílem je vytvořit unikátní obrázek, který je specifický tím, že má nadefinovanou velikost, písmo, okraje a další vlastnosti. Text spammerů se zároveň předsune před generované pozadí obrázků, kde jsou různé textury a linky. Při každém odesláni jsou obrázky drobně náhodně modifikovány, což velmi znesnadňuje detekování této nevyžádané pošty a některé metody detekce jsou úplně neúčinné.

Hojně také v poslední době roste počet podvodů typu „pump-and-dump“. Jedná se především o akcie. Jde o to, že počítačový podvodník nakoupí akcie za nízkou cenu a potom uměle zvyšuje zájem o tyto akcie rozesíláním spamu s falešnou předpovědí ohledně očekávaného růstu jejich výnosů. Studie prokázaly, že řada naivních online investorů a obyčejných příjemců nejen takový email otevře a čte, ale i reaguje. Do dvou dnů se dá prostřednictvím těchto spamů vydělat na každé akcii 5-6 procent jejich hodnoty.



Obrázek 4: Obrázkový „pump-and-dump“ spam [5]

1.3 Výdělky

Položme si pár otázek. Proč to vůbec dělají? Proč spammeři každý den obtěžují miliony uživatelů svými spamy? Za vším jsou peníze a jejich výdělky bývají nemalé. Za vším je i hodně práce, ale jak je vidět tak se jim to vyplácí a myslím si, že ještě dlouho vyplácet bude. Uvedu pár nejvíce výdělečních spammerů. První místo zaujímá Alex „Kryv" Poljakov z Ukrajiny, který odpovídá mimo jiné i za grafické spamy s bezcennými akciemi. V loňském roce přišel Poljakov se sofistikovaným malwarem SpamThru – trojský kůň/bot s vlastním antivirem, který infikuje špatně chráněné počítače, ze kterých pak rozesílá spamy. Jednotlivé kopie SpamThru navzájem spolupracují v P2P síti a mimo jiné si vyměňují statistiky o snadno napadnutelných systémech. Podle studie společnosti SecureWorks se odhaduje, že v síti SpamThru pracuje nejméně 75.000 serverů ve 170 různých zemích. [5]

	Jméno	Země	Specializace	Odhadované roční příjmy
1.	Alexej Poljakov	Ukrajina	léky, hypotéky, finance	13 mil. USD
2.	Leo Kuvajev	Rusko	„OEM" software	9 mil. USD
3.	Amichari Inbar	Izrael	porno, léky, levné akcie	7 mil. USD
4.	Ruslan Ibragimov	Rusko	cokoliv	6,7 mil. USD
5.	Nikhil Kumar Pragji	Austrálie	spam-hosting	5 mil. USD

Obrázek 5: Nejhorší spammeři

Dále bych uvedl jak si stoji země a kontinenty v distribuci spamu. [6]

Position	Country	Percentage of spam relayed
1	United States	19.8%
2	China (including Hong Kong)	7.5%
3	Poland	7.4%
4	South Korea	7.0%
5	Italy	5.0%
6	France	4.1%
7	Germany	3.7%
8	Spain	3.5%
9	Brazil	3.1%
10	Russia	3.0%
11	India	2.8%
12	Taiwan	2.5%
Others		30.6%

Obrázek 6: 12 největších producentů spamů na počátku roku 2007

Position	Continent	Percentage of spam relayed
1	Europe	35.1%
2	Asia	33.4%
3	North America	22.9%
4	South America	6.6%
5	Africa	1.4%
6	Australasia	0.6%
7	Antarctica	0.0%

Obrázek 7: Rozdělení kontinentů

2 METODY VYUŽÍVANÉ PRO ŠÍŘENÍ SPAMŮ

V současné době existují mnoho typů globální digitální komunikace. Všechny tyto komunikace mohou být potencionálně zneužity, ať už jde o jakýkoliv digitální prostředek jako například ve formě SMS, rozesílání faxů nebo elektronickou poštou. Z globálního hlediska právě internet je nejsnáze zneužitelný pro šíření spamu a to díky nejnižším nákladů pro rozesílatele, ať už právě elektronickou poštou, komunikačními programy či diskusními fóry. Spam se ale nemusí šířit jen v elektronické podobě, muže mýt mnoho různých podob, ale protože šíření spamu v elektronické podobě je momentálně nejvíce diskutabilní, tak se právě na tuto podobu zaměřím.

2.1 Elektronická pošta

Bezesporu jedním z nejstarších komunikačních kanálů mezi dvěma stranami je právě elektronická pošta. Na internetu je velmi velké množství programů, které nabízí hromadné rozesílání emailů a jejich obsluha, je velmi snadná. Jakmile adresát není s tímto srozuměn, tak se jedná o porušení zákona. Jelikož spammer nemůže k rozesílání zpráv používat svůj vlastní systém, protože by se na něj velmi rychle přišlo a okamžitě by byl blokován, tak používá cizí systém a to ten, který je založen na protokolu SMTP.

2.1.1 SMTP protokol a využití

SMTP je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP. Jedná se o jednu z nejstarších aplikací, původní norma RFC 821 byla vydána v roce 1982 (v roce 2001 ji nahradila novější RFC 2821). SMTP funguje nad protokolem TCP, používá port TCP/25.

SMTP má tři logické prvky:

- MUA - Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
- MTA - Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
- MDA - Mail Delivery Agent, program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky

zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.) [7]

Dále bych se zmínil, že spammeři používají SMTP servery, které mají povoleno doručování pošty do všech domén v internetu. Tyto servery pracují v režimu open relay (otevřený přenos) a vlastně umožňují i takové rozesílání elektronické pošty, jejímž odesílatelem ani příjemcem není autorizovaný uživatel. Tyto servery riskují, že při jejich odhalení budou okamžitě dány na černou listinu spammerů.

2.1.2 Princip rozesílání elektronické pošty

V dnešní době je realizace zasílání emailů vytvářena pomocí tří protokolů SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol version 3), IMAP4 (Internet Mail Access Protocol version 4). Všechny tři jsou součástí rodiny protokolů TCP/IP na kterých je postavený dnešní Internet. „SMTP sám o sobě slouží pouze pro spolupráci poštovní serverů. Neumožňuje autorizace, a tedy nemůže sloužit pro výběr pošty ze serverů. K tomuto je určen protokol POP3, jenž zajišťuje komunikaci mezi poštovním serverem a klientem MUA, čímž umožňuje uživatelům přijímat a odesílat poštu z, respektive na poštovní servery. Na tomto protokolu pracují klasičtí emailoví klienti např. Outlook od společnosti Microsoft. Stejnou funkci má i IMAP4, který umožňuje manipulaci s poštou, jako je vzdálená správa složek, výběrové kopírování, prohlížení záhlaví, třídění atd. Nejvíce se používá pro dálkový výběr pošty. Při používání jen jednoho počítače je lepší používat POP3.

Přenos zprávy tedy probíhá tímto způsobem: emailový klient MUA pomocí protokolu SMTP posílá poštu na emailový server, zde ji přijme MTA (Mail Transfer Agent) a následně si příjemce, pro kterého je pošta určena může zprávu pomocí protokolu POP3, případně přes IMAP4 ze serveru stáhnout. V této chvíli je email prostřednictvím Mail Transfer Agenta přesměrován na MDA (Mail Delivery Agent) příjemce, který zprávu uloží na jeho počítač. [8]

2.1.3 Opatření omezující rozesílání elektrické počty

Ve většině případů jsou spamy rozesílány distribuovaně z počítačů napadených virem. Tyto viry slouží k tomu, aby spammer mohl dálkově ovládat počítač a zneužít jej pro rozesílání spamů. Počítač se dá chránit klasickou antivirovou ochranou.

Jednou z dalších možností jak ztížit spammerům jejich šíření je nepoužívat SMTP server jako open relay. Tyto servery velmi usnadňují rozesílání a to tak, že umožňují přijmout spam odkudkoliv a taky jej kamkoliv dopravit. Často se stává, že jeden dopis bývá adresován až na stovky adres a tím snižuje zátěž na spamboota. Průchodem přes open relay se také maskuje IP adresa, což silně stěžuje odhalení spamu na straně cílového SMTP serveru. Nastavení SMTP serveru by mělo být takové, aby server nepřebíral k přepravě dopisy, které jsou zaslány z vnějšku domény a nemají adresáta uvnitř domény, kterou server pokládá za vlastní.

2.2 Komunikační programy

Mezi další prostředky, které nám umožňují lehčí práci a komunikaci, ale zároveň nám mohou dosti potrápit náš život, jsou tzv. Instant Messangery jako např. ICQ, QIP, Miranda nebo Windows Messanger atd. Tyto programy se dosti dají zneužít pro hromadné rozesílání spamových zpráv a také hlavně k vyhledávání nových emailových adres. Z vlastní zkušenosti vím, že pomocí těchto programů jde posílat široká škála nebezpečných virů. Obvykle stačí jen jednou kliknout na přijatou zprávu a váš počítač je okamžitě infikován. Proto bych se zdržel vystavování své adresy (např. ICQ number), na každé druhé stránce kterou navštívím.

Ještě bych se zmínil, že QIP, který komunikuje na ICQ protokolu, je vybaven oproti ICQ Antispam filtrem, který by měl zabránit posílání spamů a dále Anti-Flood filtrem, který by měl zabránit příliš rychlému rozesílání zpráv.

2.3 Diskusní fóra

Zde jde o trošku odlišnější druh problému, protože problém, který nastane, musí řešit provozovatel dané diskuze či fóra sám. Jedná se o to, že vlastně nemůžeme nikomu zabránit tomu, aby vložil jakoukoliv zprávu, odkaz nebo nevyžádanou reklamu, která nesouvisí z diskuzí na dané téma do příspěvku a tím zasáhnout mnohdy velké množství lidí. Bránit se před tímto druhem spammingu je mnohem obtížnější než si kdokoliv může představit. Samozřejmě existuje několik způsobů obrany.

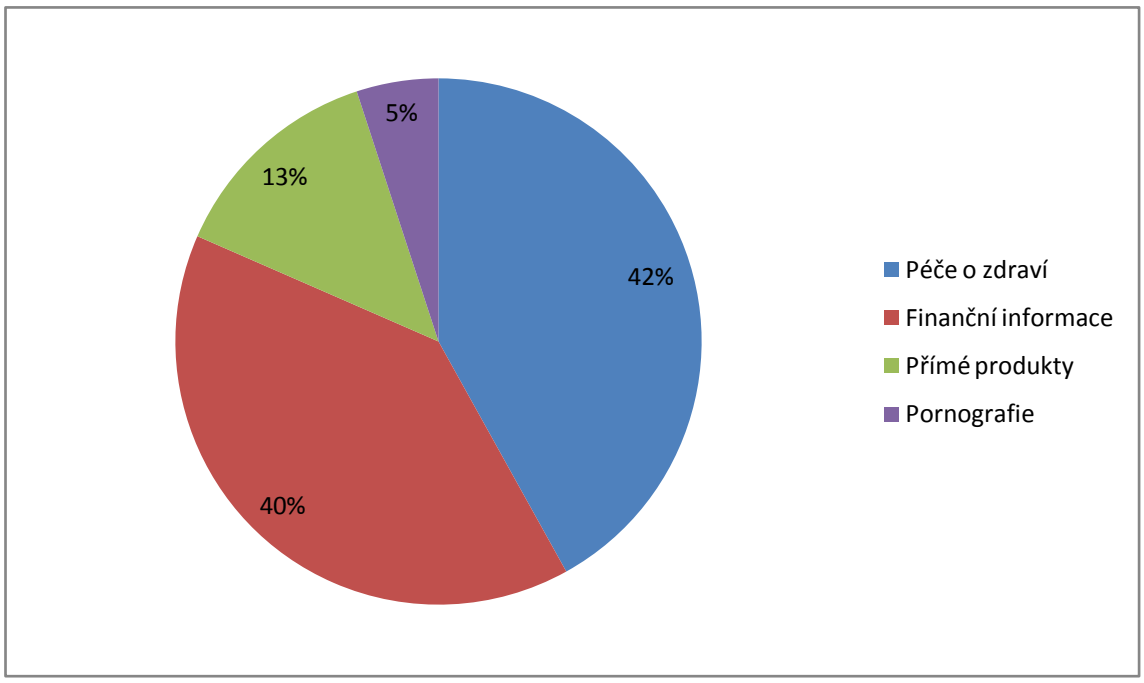
Způsob obrany s technologii Asirra z dílny Microsoft využívá obrázky bez zdeformovaných znaků. Zobrazují se nejrůznější předměty a cílem je odpovědět co se na obrázku nachází. Dům? Květina? Počítač? Tento způsob spamboti tak snadno neobejdou.

Dále to můžou být ochrany založené (např. na logice a matematice, blokováním přístupů daným uživatelům, automatické mazaní příspěvků atd.)

2.4 Obsah spamů

2.4.1 Reklama

Zaměřím na spamování pomocí emailů, protože je nejvíce používané. Základním kritériem většiny spamových zpráv je šíření reklamy, různých nabídek, propagace produktů a služeb. Toto vše je obsahem nevyžádané pošty. Zastoupení má opravdu široká škála. V poslední době je zaznamenán nárůst nabídek z oblasti finančních služeb. Podpora zákona, která by tyto nepříjemné činnosti měla minimalizovat, je bohužel nedostačující. Uživatelé, kteří spamové zprávy šíří se bohužel dokážou přizpůsobovat zákonům a tím pádem nedochází k snižování šíření spamů, ale právě naopak. Podle rozsáhlých průzkumů jedné společnosti je celosvětově 70% z přijatých emailových zpráv spam a v budoucnu je očekáván nárůst až na 80%.

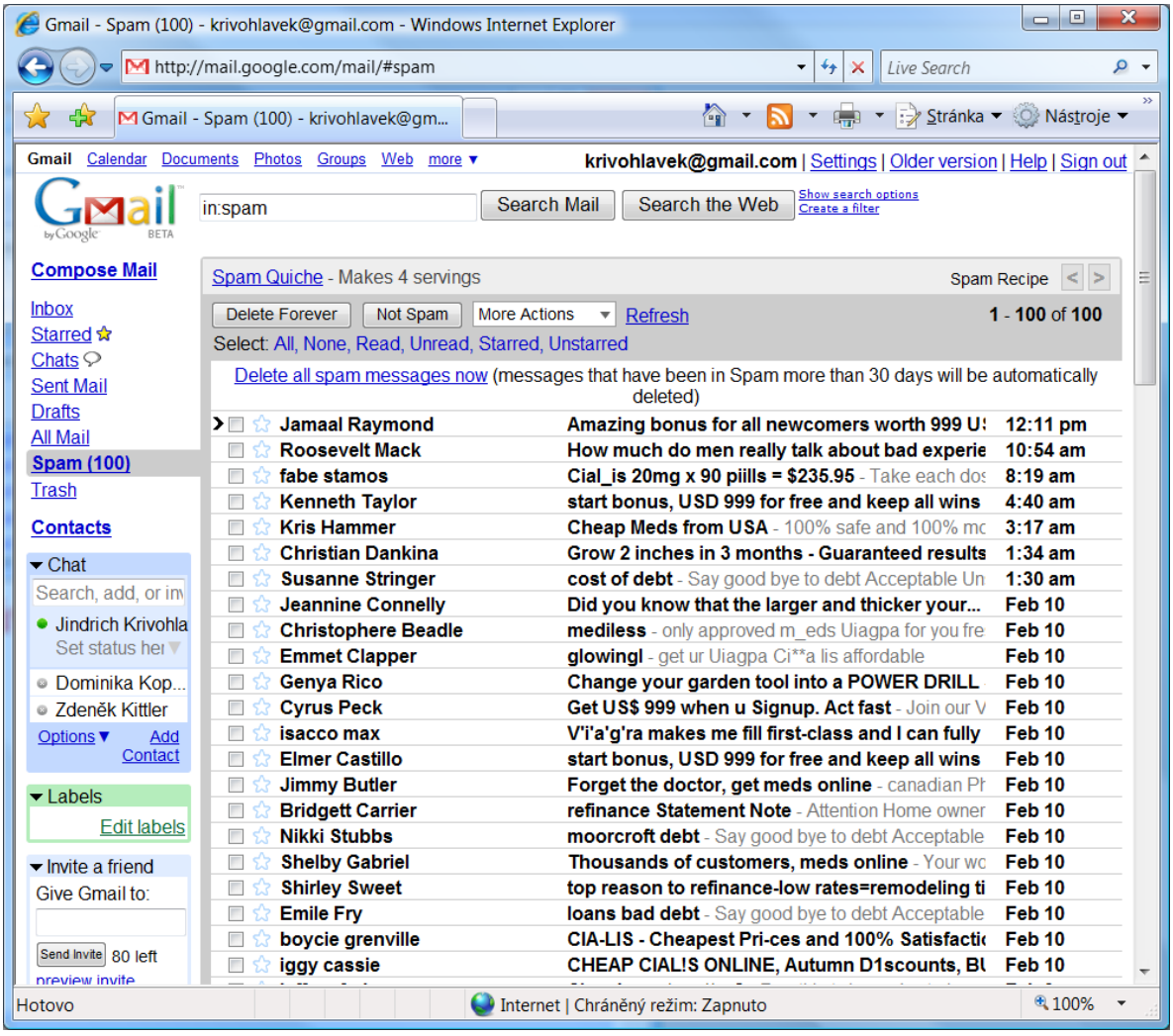


Obrázek 8: Rozvrstvení témat nevyžádané pošty (společnost Clearswift)

Dnes se společnosti zaměřují jiným směrem než na pornografii. Ta byla v žebříčku na předních místech v minulosti. Nyní se zaměřují na rozšiřování informačního finančního charakteru. Finanční typy, jak investovat na burze, náměty na levné půjčky a nebo hypotéky. Ruku v ruce s šířením informací o Viagře, neuvěřitelných dietách a přípravcích pro růst vlasů.

Předpokládané náklady celých spojených států za rok 2003 se pohybují přibližně kolem 10 miliard dolarů. Britské firmy, které nasazují ochranná opatření proti spamu již vydaly okolo 3,2 miliard liber. [9]

Uvedu příklad hojného zahlcení schránky reklamním spamem. Jedná se nejrůznější o druhy reklam od Viagry až po finance. Jak už to většinou bývá, tak jsou všechny v anglickém jazyce.

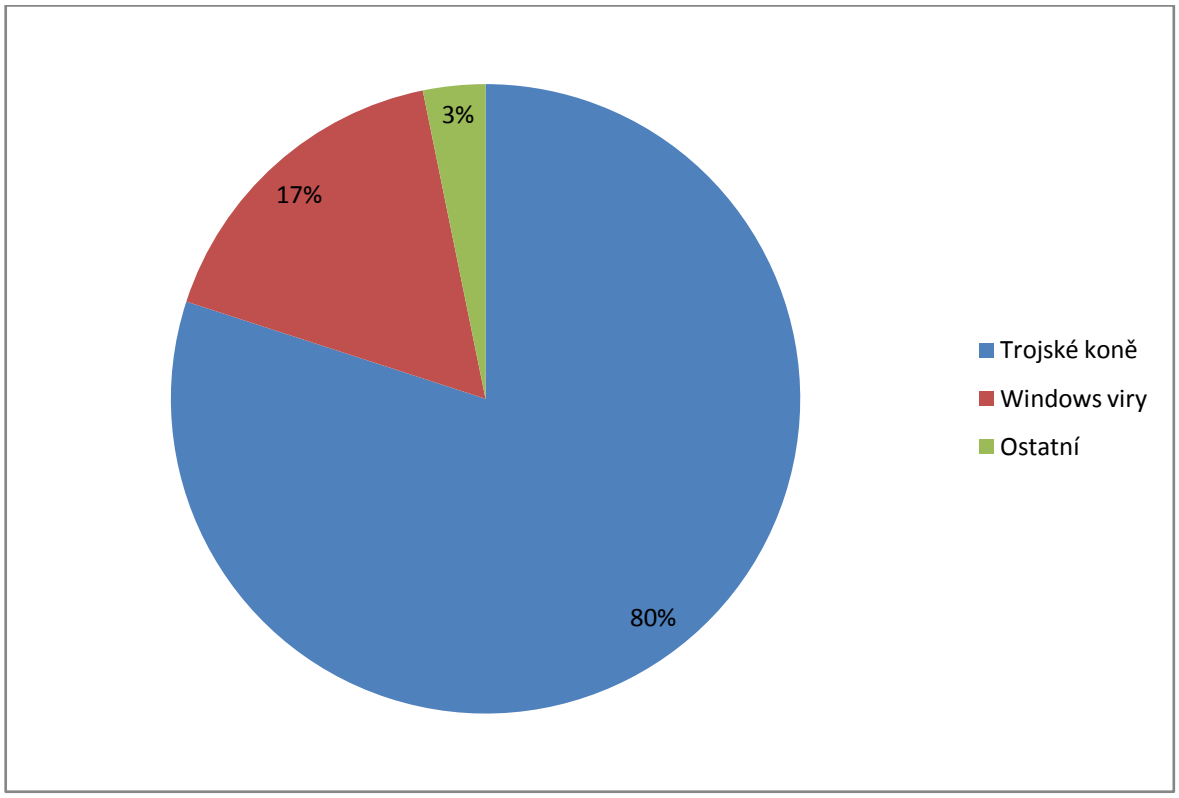


Obrázek 9: Reklamní spamy [10]

2.4.2 Viry

Jedním z druhů spamů mohou být zavirované maily. Záměry rozesílatelů takových to emailů jsou různorodé, ale jsou v podstatě stejné jako záměry těch, kdo viry píší. A to škodit druhým na úkor svých zisků a potěšení. Uvedu takové dva konkrétní účely, za kterými jsou v rozesílaných emailech viry.

Jedním z nich je získávání osobních a citlivých údajů od ostatních uživatelů za pomocí spywarů a trojských koňů. Obvykle stačí jen kliknutí v zavirovaném spamu a nainstaluje se do vašeho počítače program, který dokáže sledovat veškerou vaši činnost. Může to být navštěvování různých webových stránek, ale hlavně takových kde se zadávají hesla, jako např. pro vstup do bankovních aplikací. Což muže mít velmi katastrofální vliv na bankovní účet daného uživatele. Protože jde autorům hlavně o peníze, tvoří většinu zavirovaných emailu takové viry, které získávají hesla. Vyplívá to i z následujícího grafu

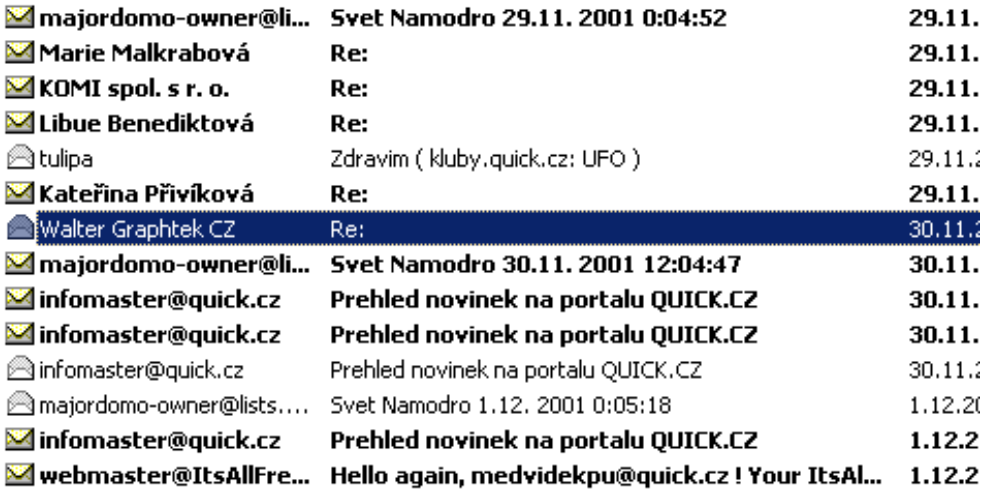


Obrázek 10: Trojské koně vs. Windows červi a viry v roce 2006

Dalším důvodem k zavirování počítače je získání jeho kontroly pro využití distribuovaného rozesílání spamů. Výhody tohoto použití jsou jednoznačné. Nepřijde se na původního šiřitele spamů, protože spamy nejsou rozesílány z jeho počítače, ale z počítače nic netušícího uživatele. Taky využívá spoustu cizího strojového času, což je výkon HW jako celku, nebo taky kapacitu datového připojení.

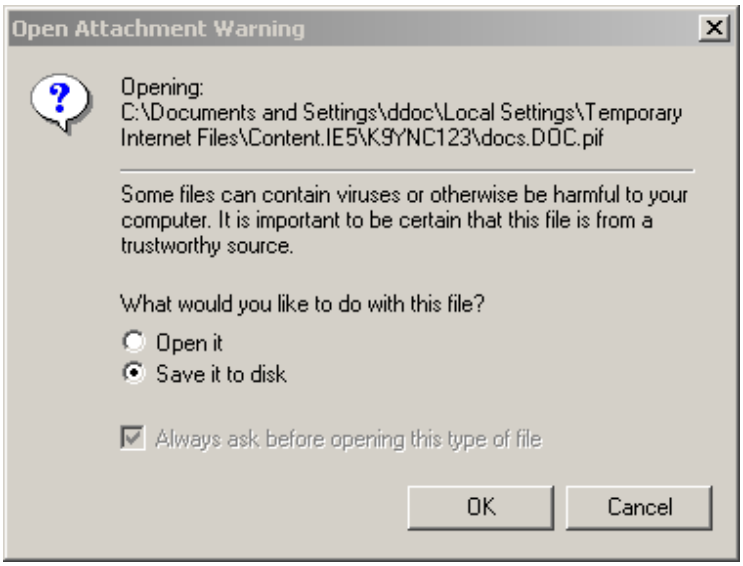
Příklad zavirovaných emailů v Outlook Express:

Všechny emaily s předmětem Re: obsahují vir. [11]



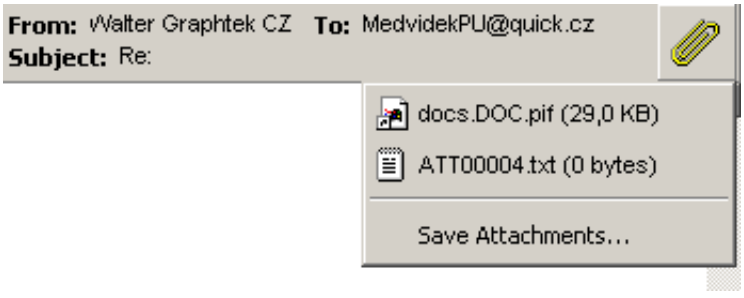
Obrázek 11: Výřez z došlých emailů v Outlook Express

Stačí otevřít nebo pouze nastavit kursor na takový email a objeví se vir. Pak už stačí jen uložit a automaticky se okamžitě vir nainstaluje do našeho PC.



Obrázek 12: Instalace viru

Samostatný email pak vypadá takto:



Obrázek 13: Samostatný email

2.4.3 Phishing

Další a velmi rozrůstající se nebezpečná činnost je tzv. phishing. Tento pojem pochází z anglického slova fishing, což znamená rybaření a řekl bych, že plně vystihuje tuto činnost, protože nic netušící uživatelé jsou chytáni na falešné emailové zprávy. Jsou to podvodné emaily, které se tváří jako pravé. Snaží se z běžných uživatelů vylákat jejich osobní, citlivé informace např. hesla, čísla kreditních karet apod. Nejčastěji to bývají stránky, které vypadají jako oficiální stránky bank a podobných institucí. Snaží se přesvědčit adresáta o tom, že se vyskytly problémy s přihlašovacím jménem a žádají, abychom zadali své údaje do předem připraveného formuláře, který byl přesně pro tento účel vytvořen.

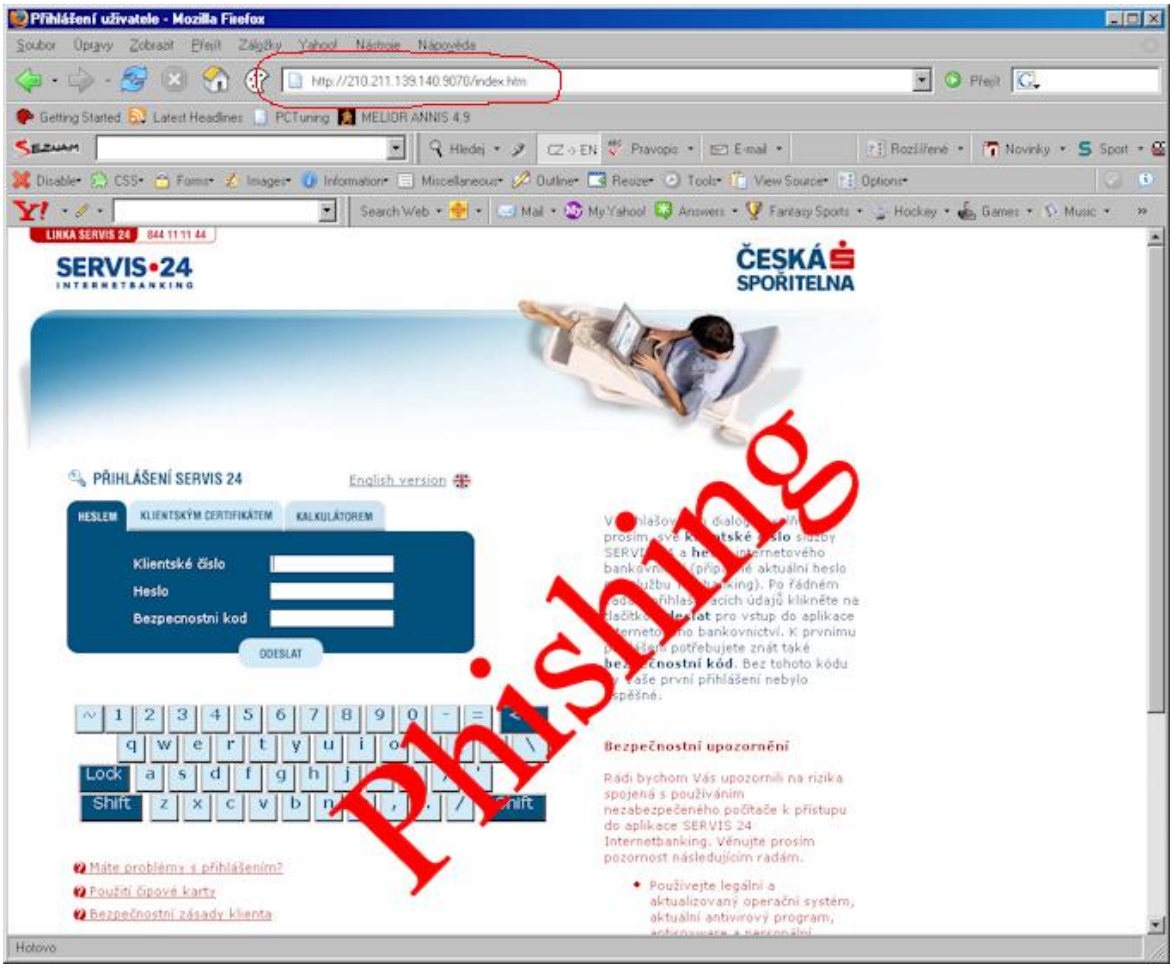
Ale tyto podvodné emaily mohou být mnohem víc propracované a tím pádem, si musíme dávat, čím dál tím větší pozor. Můžeme obdržet email s odkazem na web naší banky. Tyto stránky jsou tak důvěryhodné, že nám připadají jako pravé. Jak po grafické, tak po stylistické stránce a dokonce i obsahu, si budeme připadat jako na stránkách naší banky. Jenže se jedná o přesnou kopii. Jakmile zadáme naše údaje, tak okamžitě putují do databáze autora, který tento web vytvořil a ten se může okamžitě pokusit převést peníze na z našeho účtu na svůj nebo naše údaje někde prodat.

Takováto podvodná webová kopie se dá poznat tak, že v adresním řádku kde bývá napsaná adresa, je jinačí adresa něž je zvykem např. místo www.servis24.cz (který používá ČS) tam bude něco jako http://frag/banking.php, nebo http://130.152.11.00/index.htm).

Na první obrázku [12] uvádím příklad originální stránky České spořitelny.

Obrázek 14: Originál

Na druhém obrázku [12] je falešná stránka. Tam kdybychom zadali naše přihlašovací údaje, tak v nejbližší době budou zneužity. Na první pohled je k nerozeznání od originálu. Všechno co má originální stránka je i tady, grafika je taky dokonalá. Jediný rozdíl je v adresním řádku. Podle toho zaručeně poznáme, jestli jde o falešnou stránku nebo originál.



Obrázek 15: Phishing

Riziko je u nás velmi reálné. Na jaře 2008 dlouhodobě probíhaly soustavné phisingové útoky na zákazníky České spořitelny. Zpočátku byly falešné zprávy snadno odhalitelné, podle nedůvěryhodného strojového překladu zprávy do češtiny, do kterého pronikly i srbochorvatské znaky nebo cyrilice, ale později začaly phishingové zprávy využívat text varování před phishingem, které sama Česká spořitelna uvedla na svých webových stránkách, což emailové phisingové zprávy činilo nebezpečnějšími.

Platí zde klasické zásady obrany:

- Nesdělujte nikomu heslo (ani ho nikam neposílejte emailem).
- V případě bankovních služeb neklikejte na odkazy v nevyžádané emailové zprávě.
- Kontrolujte v adresním řádku (nahoře) prohlížeče, zda nejste na jiném serveru, než chcete být nebo než tvrdí obsah stránky (text, logo, grafika, …).

- Vhodné je heslo zadávat přes klávesnici na obrazovce, pokud ji portál nabízí, protože klikání myší se v případě napadení počítače monitoruje obtížněji, než zadávání textu. [A]

3 NEJČASTĚJŠÍ ZPŮSOBY ZÍSKÁNI ADRES

Existuje široká škála, jak spammeři do svých databází získávají emailové adresy. Popíši ty nejběžnější a nejpoužívanější. Řekl bych, že v určitých případech je získání adres pro spammery velmi jednoduché, protože jim to lidé hodně usnadňují. Uživatelé nevědomky přímo vystavují své adresy na webech a tím pádem si spamové zprávy skoro objednávají.

3.1.1 Pozor při registracích

Základním způsobem, jak se dostávají naše adresy do rukou spammerů je registrace uživatele. Úplně nejhorší jsou servery s nedůvěryhodným obsahem. Jsou to z pravidla zahraniční servery s obsahem na hranici slušnosti nebo dokonce zákona. Při registraci na těchto serverech a vystavení naší emailové adresy ji dobrovolně dáváme spammerům a brzy můžeme očekávat příval spamů do naší emailové schránky. Opravdu nedoporučuji na takových serverech něco uvádět.

Samozřejmě ani využívání služeb důvěryhodných serverů není stoprocentní, ale riziko se několikanásobně snižuje. Platí to jak u zahraničních tak u českých webových portálů.

Zadávat při registraci neexistující emailovou adresu rozhodně řešení také není, protože provozovatel serverů zasílá na zadanou adresu potvrzovací kód, který je nutný k aktivaci účtu. Důvod není ten, že bych chtěl distribuovat spam, ale např. při zapomenutí hesla ho mohou poslat zpět na naši adresu. Proto bych doporučoval založit si emailovou adresu, která bude určená pouze pro registrace na webových portálech.

3.1.2 Zveřejněním – spamový roboti

Emailové adresy jsou do spamových databází získávány pomocí tzv. spambotů, kteří prochází internet a sbírají vystavené emaily. Tento způsob sbírání adres je velmi populární a hlavně rozšířený. Spambot dokáže nalézt adresu uvedenou i jako obyčejný text. Nezabývá se něčím nepodstatný, ale jen sbíráním emailový adres. Sbírá vše, co vypadá jako adresa, tzn. textový řetězec obsahující zavináč a tečku. Proto se zavináč a tečka přepisují doslovně (např. jmeno(dot)přímení(zavináč)portal(tecka)cz). Tento způsob zápisu adres začíná být stále populárnější a začíná se rozšiřovat. Předpokládá se, že někteří spamboti si s ním už brzy poradí. Řešením by bylo nahrazení adresy nebo její části obrázkem. Sice rozeznání obrázku už dávno není problém, ale pokud se ještě stále ve většině případů používá textové uvádění adres, tak by to bylo plýtváním strojového času.

3.1.3 Obyčejnou existencí - Freemaily

Pouhé založení emailového účtu stačí k tomu, aby se začal plnit nevyžádanou poštou, a přitom tento účet nemusí vůbec nikdo používat. Některé méně seriozní freemailové servery totiž dokážou zvyšovat své příjmy pouhým doručováním spamu do schránek svých uživatelů.

Jeden server svého času doručoval svým uživatelům reklamní poštu od nejmenovaného operátora, ale měl aspoň tolik slušnosti, že všem uživatelům založil konkrétní složku, aby se nemíchala s běžnou poštou.

4 OBRANA PROTI SPAMU

V dnešním digitálním světě se bohužel nedá říct, že by existovala stoprocentní ochrana před spamovými zprávami a asi ani nikdy existovat nebude. Existuje však několik přístupů, které nám pomohou problémy v dané oblasti alespoň zmírnit. To ovšem už záleží na nás uživatelích, jak se budeme na internetu chovat.

4.1 Prevence

Mezi nejzákladnější obrany proti spamu patří prevence. Jedním z pravidel je nikdy se neregistrovat na stránkách s pochybnou důvěryhodností, a když už, tak aspoň nevystavovat svou primární adresu, která je používána pro soukromé, či pracovní účely. Dalším z pravidel je nevystavovat emailovou adresu na diskusních fórech nebo kdekoliv na internetu. Přece jen když ji chcete uvést, tak používejte tvary, se kterými si roboti neumějí moc poradit (např. jméno(zavinac)domena(dot)cz). Jako tvary se používají české nebo anglické výrazy. Neméně důležitým pravidlem je nikdy neodpovídat na pochybnou poštu nebo navštěvovat odkazy v ní uvedené. Za pochybnou poštu lze považovat takovou, která přišla z námi neznámého zdroje nebo v cizím jazyce. Drtivá většina spamů bývá v anglickém jazyce.

Rozesílatelé spamových zpráv mají velké množství cest, jak se dostat k našim emailovým adresám.

4.2 Filtry

Filtrování pošty lze rozdělit do dvou úrovní, buď to na straně poštovního klienta, nebo přímo na serveru. Obě metody mají kladné a záporné stránky. Všechny tyto metody rozvedu dále.

4.2.1 Filtry na úrovni poštovního klienta

4.2.1.1 Programy

Antivirové či antispamové programy se starají o filtrování příchozích emailů na straně klienta nebo se také dají nastavit filtry přímo v poštovním klientovi (např. Outlook). Existují také programy, které lze doučit program případné nesrovnalosti. Tato metoda je flexibilní a přístupná, ale má pár nevýhod.

- Klient ze serveru musí stáhnout část zprávy, což pro uživatele, kteří používají telefonní připojení muže být obtěžující, ale v dnešní době si myslím, že takových uživatelů už není mnoho.
- Je skoro nemožné zjisti, zda všichni uživatelé na nějaké rozsáhlé síti mají stáhnuté aktuální antivirové a spamové databáze.

4.2.1.2 Bayesovské filtry

Bayesovské filtry neblokují příchozí poštu podle IP adresy, ale podle dané zprávy. Pravděpodobně se uživateli nedoručí takový email, ve kterém se bude vyskytovat určitě množství vybraných klíčových slov. Tyto filtry využívají triky z oblasti umělé inteligence. Základním principem fungování těchto programů je spolupráce s uživatelem, který těmto programům sdělí, zda emailový zpráva je spam nebo nikoliv. Zprávy jsou tříděny na spamové a hamové (ne spamové). Porovnává klíčová slova, která jsou ve spamové poště a přiřazuje jim určitou váhu. Ze začátku se bayesovské filtry učí převážně od uživatele, ale jakmile získají dostatečně velkou databázi klíčových slov, tak už si pak vystačí samy. Matematik Thomas Bayes sestavil vzorec, kterým si tyto filtry vypočítávají pravděpodobnost. Výpočet této pravděpodobnosti v podstatě funguje tak, že si z emailů program vytáhne slova a u každých zvlášť spočítá pravděpodobnost, že je emailová zpráva, ve kterém se nachází podezřelé slova spamem. Výpočet se počítá jako podíl všech spamových zpráv kde se dané slovo nachází, ku počtu všech zpráv, kde se slovo vyskytuje.

Spammeři ve většině svých emailů používají slova jako Viagra a to v nejrůznějších tvarech (VIAGRA, viagra!!!, Viagra!) a proto je bayesovská metoda proti nim velice účinná, protože filtry tyto slova dokážou velmi snadno rozpoznat, jelikož se v hamový na rozdíl od těch spamových emailech až tak často nevyskytují. Je nutné porovnávat i další klíčová slova, protože se slova jako Viagra můžou vyskytovat i v hamových emailech.

Dalším často se vyskytujícím slovem v obou případech emailů jsem slovo money. Ve snaze obejít filtry se spammeři v poslední době snažily přicházet s novými věcmi a začali slovo money modifikovat na tvar slova m0ney. Mělo to paradoxně opačný účinek a filtrům to práci usnadnilo, protože takovéto slovo se v běžných hamových emailech nevyskytne snad vůbec. Dále se věnuje obrovská pozornost i URL odkazům, které se ve zprávách vyskytují, popřípadě se za velmi kritické a nebezpečné emaily označují ty, které jsou celé napsané v HTML. Bayesovské filtry jsou pro praxi velice účinné a mají řádně propracovaný systém, avšak jednou vetší nevýhodou je délka počátečního učení, kdy si program získává svou databázi klíčových slov. Uživatelé v neanglicky mluvících zemích však mají obrovskou výhodu, protože většina spamu je napsána v anglickém jazyce a bayesovský filtr si velmi brzo přiřadí k anglickým slovům velkou spamovou pravděpodobnost.

Uvedu zde první a druhý Bayesův vzorec: [13]

$$P(H_k|A) = \frac{P(H_k).P(A|H_k)}{\sum_{i \in I} P(H_i).P(A|H_i)}$$

Obrázek 16: První Bayesův vzorec

Zde se ptáme na pravděpodobnost jevu, který je totožný s jednou z hypotéz H.

$$P(B|A) = \frac{\sum_{i \in I} P(H_i) \cdot P(A|H_i) \cdot P(B|A \cap H_i)}{\sum_{i \in I} P(H_i) \cdot P(A|H_i)}$$

Obrázek 17: Druhý Bayesův vzorec

Zde se ptáme na pravděpodobnost jevu, který je zcela nový a nesouvisí s ostatními popsanými jevy.

4.2.2 Filtry na úrovni serveru

Filtrování na úrovni MDA v podstatě řeší jeden základní problém. Nevyžádanou poštu ničí přímo na serveru a to tak, že ji odstraní dřív než by si ji uživatel mohl stáhnout. Na druhou

stranu tady bohužel neexistuje přímá vazba s uživatelem, protože MDA se jej neptá, zda je tento email v pořádku, ale prostě ho smaže. Nebo když vyhodnotí, že je nějaký email podezřelý, tak pošle zprávu uživateli a ten je pro změnu otravován oznámením o spamu místo spamem. Toto řešení se mi nezdá moc praktické.

Filtry na úrovni MX

Protože nemůžeme důvěřovat adrese odesílatele, nastupuje vyšší vrstvě zpracování. Pokud nastane filtrování na MX úrovni, bavíme se přímo s MTA na nějakém serveru. Ať už je to opravdový MTA, nebo spam rozhraní, a nebo virus.

SMTP pracuje na základě zodpovědnosti za zprávy. Server příchozí zprávu uloží na disk a potom danému MTA oznámí potvrzení o přijetí. MTA odesílající zprávu ji nyní může bez obav odstranit z odchozí fronty zpráv.

Pokud není z nějakého důvodu přijetí zprávy potvrzeno (ať už je to důvod nedostatku diskového prostoru, pádu systému, vysoké zátěže, neznámého příjemce, a nebo chybě na síti), zpráva zůstává dále u odesílatele, který je zodpovědný za její doručení. Pokud je chyba jen dočasná, odesílatel se pokusí o doručení později. Když se to nepodaří vůbec, je odesílatel informován o nemožnosti doručení.

Pokud je odmítnuta zpráva přicházející ze spamovacího rozhraní, většinou není naprogramováno ošetření chyb. Nevyžádaná pošta se má šířit do celého internetu a tak jej nedoručení moc nezajímá. To je pozitivní.

Pokud je odesílatelem reálný MTA, tak je doručeno oznámení o nemožnosti doručení zprávy.

Samozřejmě, že i v tomto případě máme několik omezení, na která narazíme:

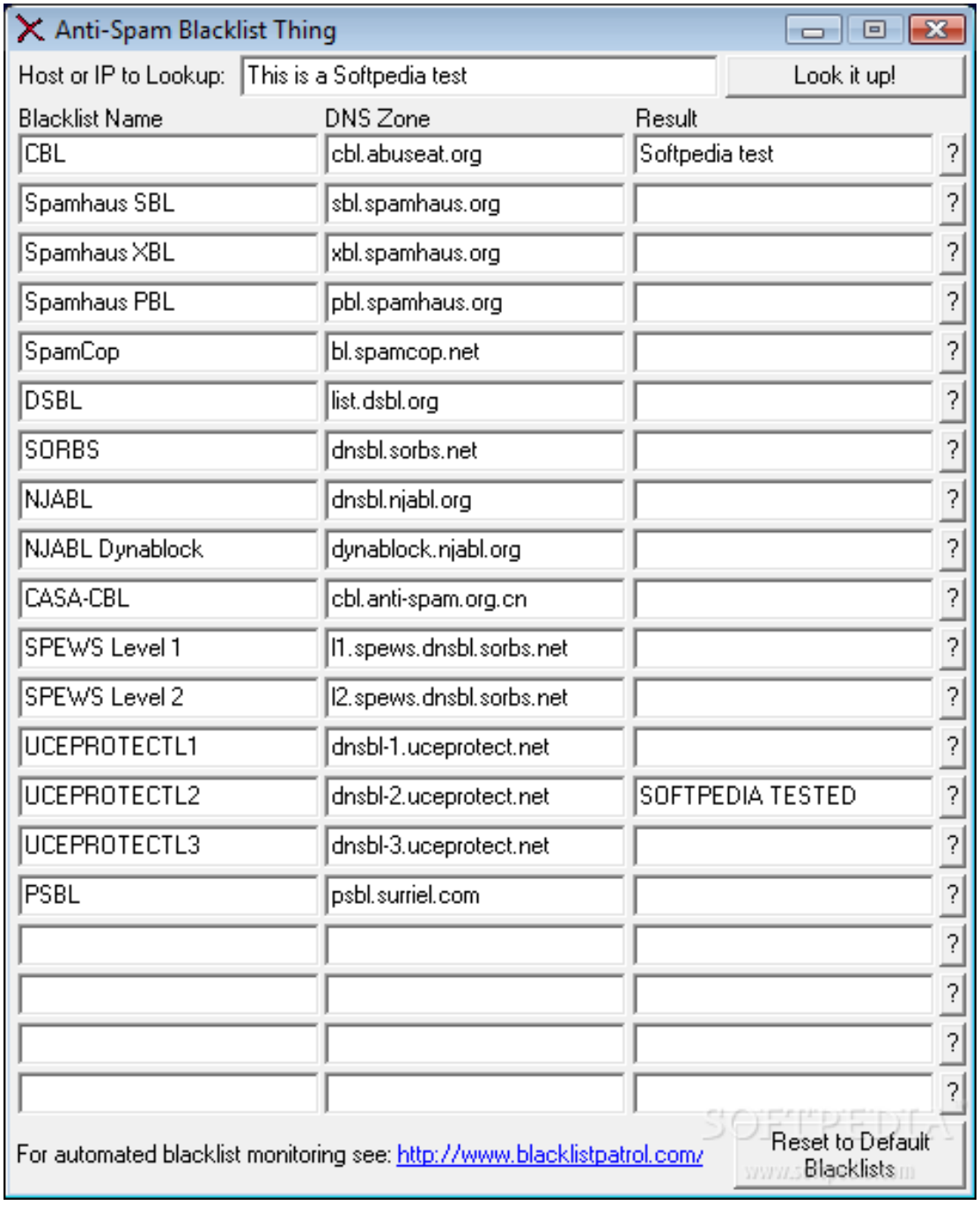
- funguje to pouze na MX úrovni, pokud je email akceptován nelze jej už na nižších úrovních odmítnout
- pokud je spam nebo vir zaslán do emailové konference, kde jeden z účastníků má filtrování na MX úrovni, tak oznámení o nedoručení obdrží administrátor konference. (řešením je emaily tohoto typu v konferenci zahazovat)
- stejný problém nastává i v případě, pokud je email přeposílán. Řešení je nyní na serveru, který email přeposílá. [9]

4.2.2.1 Blacklisty

Velice efektivní, účinnou a hojně používanou metodou v blokování nevyžádané pošty jsou tzv. blacklisty, tedy černé listiny. V oblasti počítačů a internetu se pojem blacklist užívá k označení seznamů serverů, nebo přesněji řečeno jejich IP adres, ze kterých se nedoporučuje přijímat emaily, z důvodu, že často slouží k rozesílání nevyžádané pošty. Blacklisty jsou jednou z prvních antispamových metod, která se začala používat v hojnější míře a používá se dodnes. Na začátcích spammingu používali spammeři k rozesílání nevyžádané pošty svých vlastních počítačů, tak bylo velmi jednoduché blokovat tyto zprávy přidáním IP adres jejich počítačů na černou listinu. Dnes je bohužel situace úplně jiná. Spammeři vymýšlí nejrůznější techniky jak docílit svého. Pro rozesílání nevyžádané pošty používají počítače spamem napadených uživatelů. Tyto se mění bohužel velmi rychle a blacklisty nedokážou takto rychle reagovat a aktualizovat své databáze. Řešit se tento problém dá různě, třeba pokud je z daného počítače za týden poslán spam více jak třikrát, tak se teprve poté zapíše na černou listinu. Musím dodat, že z těch počítačů, které jsou na černé listině, se blokuje úplně veškerá pošta i ta, která spamem není.

Blaklisting se rozděluje na lokální a distribuovaný. Lokální blacklist je takový, kdy se administrátor stará o seznam IP adres, ze kterých jsou spamové zprávy rozesílány. Tato technika se používá u serverů, které jsou open relay, nebo pro nováčky spammery, kteří ještě neví jak spam distribuovat. Ale zase na druhou stranu je dost těžké udržovat tento seznam aktuální, protože se odesílatelé spamu pohybují velmi rychle po internetu a ještě nepoužívají stejnou IP adresu pro odesílání zpráv do stejné domény.

Distribuovaný blacklist je vzájemné sdílení černých listin nejrůznějších serverů. Tady, ale narážíme na jeden problém. To co se muže považovat za spam na jiném serveru už nemusí být spamem také pro vás. Navíc jsou distribuované blacklisty náchylné k DOS útokům. Jsou to útoky, které jsou namířeny proti serverům nebo proti celým sítím. Jejich cílem je ochromit provoz tohoto serveru na základě zvýšení počtu přicházejících požadavků. Při takovýchto útocích hacker spustí nějaký program, aby generoval nějaká nesmyslná data a posílal je na server. Na serveru pak z pravidla dochází k zahlcení těmito daty a to znemožňuje reagovat na požadavky běžných uživatelů. V horším případě může dojít až k havarování nebo zhroucení celého systému.

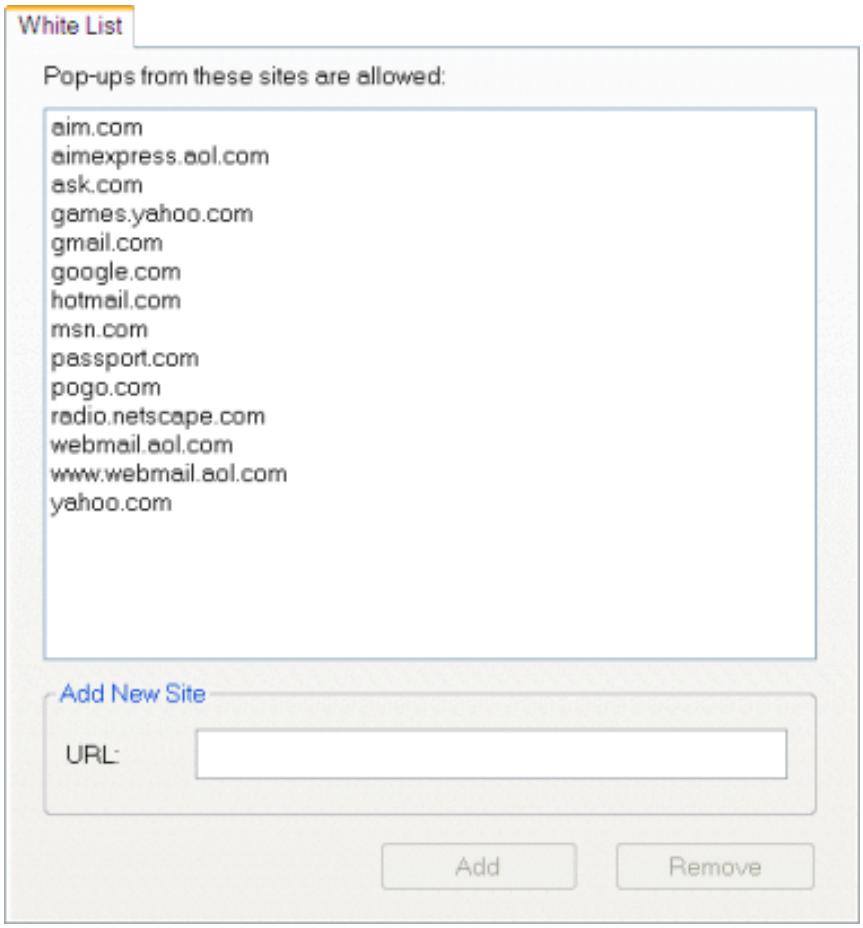


Obrázek 18: Antispam blacklist [14]

4.2.2.2 Whitelisty

Servery, které bývají velmi zatěžovány nevyžádanou poštou, mohou používat přesný opak blacklistů. Tyto bílé listiny nepoužívají seznam zakázaných IP adres, ale naopak si vytvoří seznam důvěryhodných adres, ze kterých je bezpečné poštu přijímat a rozesílat k příjemcům. Zbytek internetu je pro ně nezajímavý a tak to odstraní 100 procent

nevyžádané počty z ostatních serverů. Bohužel to ale taky odstřihne server od případných potencionálních zákazníků a kontaktů, kteří nejsou na bílé listině.



Obrázek 19: Whitelist [15]

4.2.2.3 Greylisty

Greylisting je relativně nová metoda ochrany a její hlavní myšlenkou je, že spammeři nikdy neposílají zprávu podruhé, když napoprvé je odmítnuta s nějakou dočasnou chybou. Tato metoda funguje na principu dočasného odložení přijetí dopisu. Zni to relativně primitivně, ale v kombinaci s dalšími metodami je tato metoda velmi účinná. Greylistin využívá pravidla SMTP a pokud se s MTA nepodaří doručit zprávu do příchozí pošty příjemce, tak ji uloží do tzv. Message store a tam ji drží max. po dobu dvou hodin, kde se snaží v určitých po sobě se opakujících intervalech poštu doručit znovu. Po uplynutí této doby se emaily, které se nepodařilo doručit a které tam zbyly, zahodí. Drtivá většina spammerů používá specializovaný program, jehož úkolem je co nejrychlejší rozesílání zpráv, ale jakmile se první pokus nepovede, tak podruhé se už o to nesnaží. Značná část spamu odpadne právě při tomto prvním pokusu, protože zůstane ve frontě a jelikož se o

další doručení nesnaží, tak bývá navždy smazána. Velkou výhodou je, že tato metoda šetří značné množství přenosové kapacity sítě, protože zpráva je odmítnuta už v počáteční fázi komunikace (hlavička dopisu) a samotné tělo zprávy se tedy vůbec nepřenáší. Greylisting má bohužel i velkou nevýhodu a to, že dochází ke zpoždění doručení jakékoliv pošty, tedy i té která spamem není. Tvůrci této metody na tento problém ale myslely. Aby se nestávalo, že bude zdržována pošta od známých příjemců, tak si greylisting vytváří své vlastní speciální databáze, kde si ukládá IP adresy odesílatele, jméno odesílatele a SMTP hlavičky emailu. Všechny příchozí emaily jsou porovnávány s touto databází, a pokud jde o známého odesílatele, tak poštu nepodrží a hned ji doručí. Tato metoda se při troše námahy obejít dá, tak proto autoři nedoporučují ji mít jako hlavní filtr, ale doporučují tuto metodu používat jako doplněk k jinačím metodám, jako jsou antispamy, či blacklisty.

Závěrem této kapitoly bych řekl, že bránit se proti spamu není až tak jednoduché a stoprocentní ochrana asi opravdu nikdy existovat nebude. V soukromém boji proti spamu je důležité dodržovat prevenci, opatrnost a hlavně používat a pravidelně aktualizovat antispamvé programy a kombinovat je s nejrůznějšími metodami obran.

II. PRAKTICKÁ ČÁST

5 SROVNÁNÍ BEZPEČNOSTNÍCH SW PRODUKTŮ PROTI SPAMU

Otestuji některé vybrané antispamové programy a to buď placené nebo freewarové vezre (zdarma verze). Navíc ještě otestuji program pro kompletní řešení zabezpečení počítače, ve kterém je mimo jiné i antispam.

5.1 Placená verze antispamové ochrany

Základní rozhraní:

Obrázek 20: základní rozhraní

Otestuji program s názvem SPAMfighter, je to placená verze, která bude funkční po dobu 30 dní. Je nástrojem pro Outlook, Outlook Express, Windows mail a Mozilla Thunderbird, který velmi efektivně a automaticky filtruje poštu od spamů a phishingu. Nabízí i ochranu pro více emailových účtů. Velkou výhodou je, že je program v českém jazyce a nabízí i mnoho cizích jazyků. Vybral jsem jen tento program, protože od začátku se mi zdál a velké profesionální úrovni a byl snadno ovladatelný. Hned po instalaci nám program nabídne

automatickou aktualizaci na nejnovější verzi, což přináší vyšší stupeň zabezpečení a nástroj, který se skládá ze tří kroků pro minimizování spamu.

Obrázek 21: tři kroky

- Firewall detekce: Váš firewall je prověřován, protože SPAMfighter potřebuje komunikovat se svým serverem, aby mohl filtrovat spam emaily. Jakmile nejsou zjištěny žádné problémy s firewallem, tak se SPAMfighter úspěšně spojí se svým serverem.
- Jestliže už jsme někdy v minulosti používali SPAMfighter, tak nám program nabídne použít účet, který už byl v minulosti vytvořený, nebo nám nabídne zcela nový učet pokud SPAMfighter používáme poprvé.
- Automatická konfigurace našeho whitelistu. Program automaticky prověří a vyhledá naše kontakty a přidá je na bílou listinu schválených uživatelů, což si myslím, že je velmi dobrá věc.

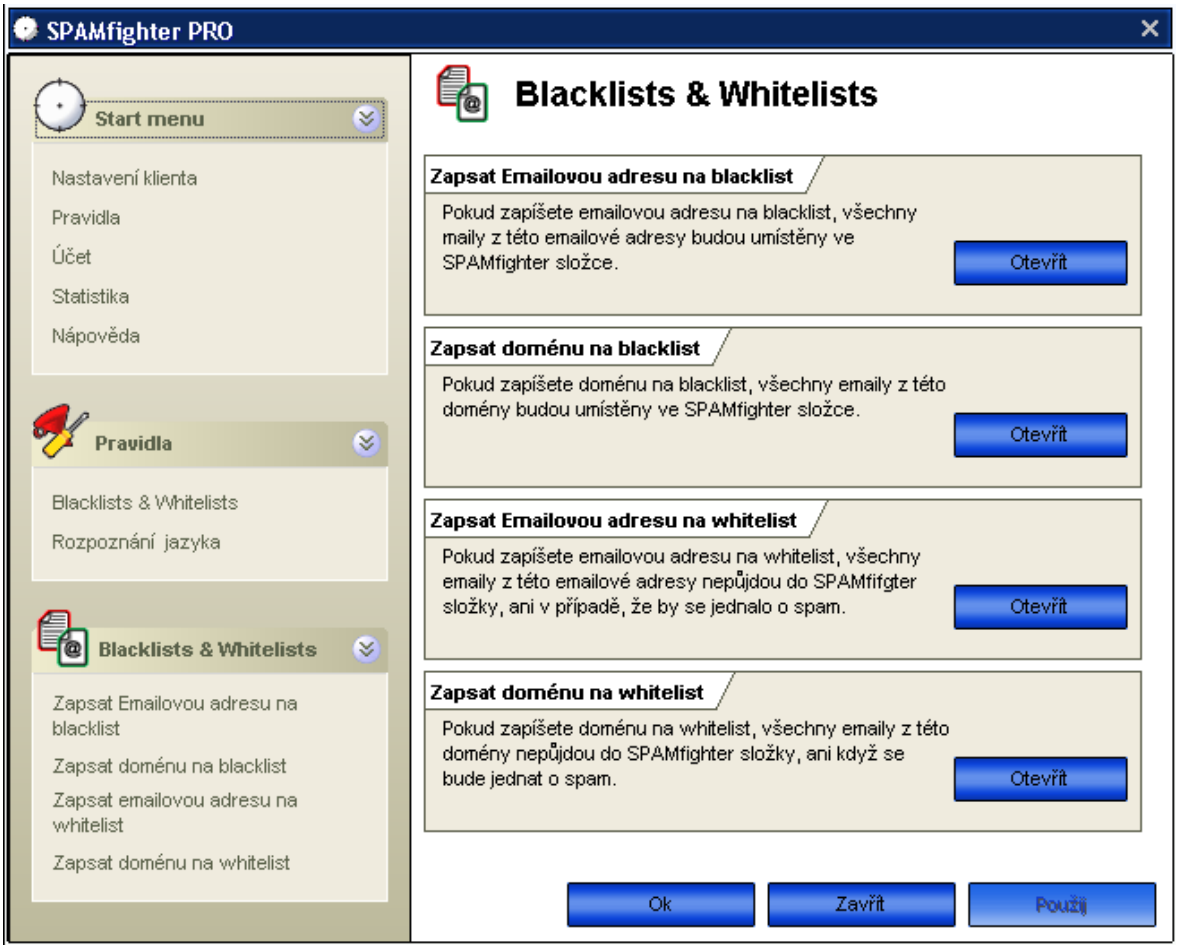
Po dokončení všech těchto kroků a úspěšné instalaci nám program nabídne odkaz na oficiální stránky programu, kde se spustí jednoduchý průvodce pro začátečníky. Za zmínku stojí opravdu velký výběr jazyků.

Zaměřím se na Outlook Express. V Outlooku se nám po nainstalování programu SPAMfighter objeví nová lišta s nejrůznějšími funkcemi.

Obrázek 22: SPAMfighter lišta

Za výhodu tohoto programu bych označil velkou jednoduchost. Tento program filtruje 95% příchozí pošty a podezřelé emaily automaticky přesouvá do speciální složky s názvem SPAMfighter, kterou si program automaticky vytvořil. Do doručené pošty se, ale také mohou dostat emaily, které tam nechceme např. reklamní nabídky nebo pošta, která se dostane přes filtr. Jednoduše se dají z doručené pošty nadobro odstranit. A to kliknutím na námi vybraný email a pak už jen stačí kliknout na tlačítko blokovat. Hned se takový email přesune do naší speciální složky SPAMfighter a další emaily ze stejné adresy už budou chodit jenom sem. Funguje to i naopak. Někdy se stane, že se do SPAMfighter složky dostane i normální email a my chceme, aby nám chodil do doručené pošty. Pak stačí kliknout na tlačítko odblokovat a emaily z této adresy budou chodit přímo do doručené pošty. Je velmi důležité používat tlačítka blokovat a odblokovat, aby se SPAMfighter naučil, co je pro nás spam a co ne. Taková to funkce nám velmi zjednoduší orientaci a filtrování naší pošty.

Filtrovat poštu také můžeme pomocí blacklistu. Přidáním emailové adresy nebo domény na blacklist bude okamžitě zamezeno přijmutí jakéhokoliv emailu. To nám usnadní také hodně práce se spamem. Pokud ale budeme chtít, aby některé příchozí emaily nebyly filtrovány a to z důvodu, že se jedná o důvěrné zdroje nebo přátele, tak jejich adresy přidáme na tzv. bílé listiny. To zamezí filtrování těchto emailů a takový email se okamžitě objeví v doručené poště.



Obrázek 23: Blacklist & Whitelist

Dalším obrovským plusem co mě zaujalo je filtrování pošty pomocí rozpoznán jazyka. Filtr lze nastavit tak, aby propouštěl emaily třeba jen v jednom jazyce nebo v jazycích, které nastavíme. K dispozici máme 28 jazyků z celého světa. Filtr jde nastavit i naopak a to tak, aby nepropouštěl emaily z jazyků, které jsme vybraly. Většina spamů je totiž zatím v cizích jazycích. Třeba z Ruska jich pochází velmi hodně, tak nastavíme filtr, aby nepřijímal emaily v ruském jazyce, což znamená azbuka. Okamžitě je po problému. Velice zajímavá a užitečná věc. SPAMfighter dokonce detekuje i obrázkové spamy.

Obrázek 24: Rozpoznání jazyka

Našel jsem asi jen jeden maličký nedostatek. On to vlastně ani asi nedostatek není. Jakmile byl SPAMfihter spuštěný a aktivní, tak jsem nikde nenašel jak ho vypnout. V praxi to znamená, že program běží po celou dobu co je zapnutý počítač. Vlastně nám to přináší nepřetržitou ochranu na emailové schránky.

SPAMfighter je profesionální program na vysoké úrovni, který zaručeně dokáže chránit uživatele před nevyžádanou poštou. Zdůraznil bych, že vše se nastavuje automaticky a vše běží bez sebemenších problémů. Nákupní cena programu je okolo 680Kč, což si myslím, že je velmi seriózní a odpovídá to kvalitám programu.

5.2 Freewarové verze antispamové ochrany

Jelikož mě nijak silně ani jedna freewarová verze neoslovila, tak jsem se rozhodl jich otestovat více. Dalším z důvodů bylo, že všechny byly hodně podobné a lišily se opravdu jen v maličkostech. Nenašel jsem ani jednu freewarovou verzi s českým jazykem, všechny

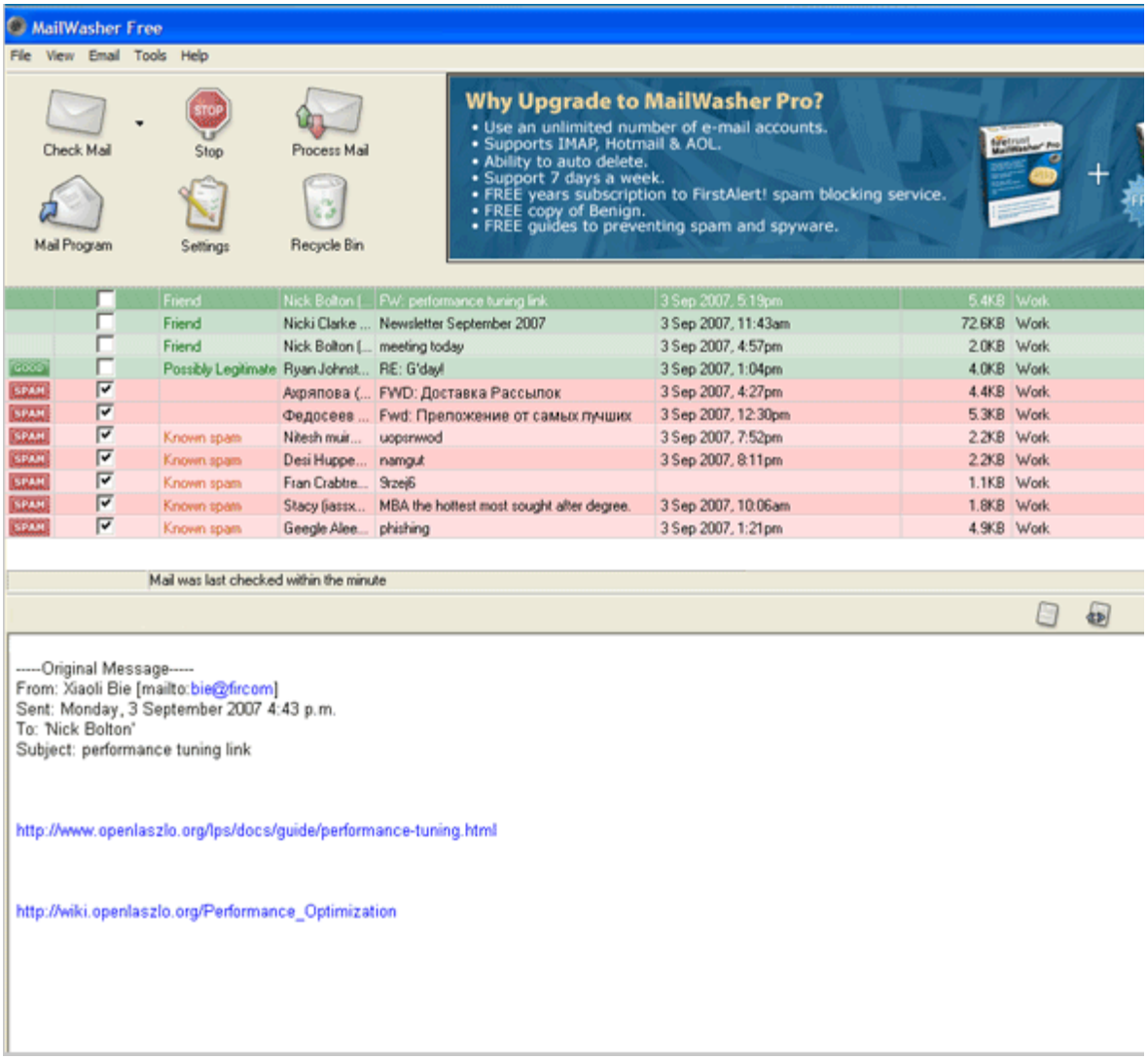
byli v angličtině. Pro uživatele, kteří neumí vůbec anglicky, to může být velký problém, protože se vše nastavuje ručně, na rozdíl od placené verze.

5.2.1 MailWasherFree

Tato verze antispamového programu je zcela zdarma, ale bohužel není v češtině. Jelikož se všechno nastavuje ručně, může to být velice problematické, pro lidi, kteří neumí moc dobře anglicky. Po nainstalování programu se musí ručně nastavit emailový účet, který bude kontrolován. Jakmile se všechno nastaví, začne kontrola naší emailové schránky. Obrovské plus tohoto programu vidím v tom, že filtruje poštu přímo na serveru. Pošta je tím pádem kontrolována ještě dřív než ji vůbec stáhneme do PC. Dle svojí databáze dokáže i rozpoznat zavirovanou poštu. Filtr pracuje na vlastních i externích blacklistech. Jednoduše si můžeme nadefinovat svoje vlastní blacklisty a podporuje i definice whitelistů. Vedle základních možností odstranění nevyžádané pošty je tu ještě jedna speciální možnost. Jelikož kontrola spamu je prováděna přímo na serveru a pošta se okamžitě nestahuje do PC, tak jde spam poslat zpět odesílateli v takovém formátu, že to vypadá, že naše emailová adresa neexistuje (tzv. bouncing). V tomto vidím sílu tohoto programu, protože spammeři většinou neposílají dvakrát spamové zprávy do neexistujících adres. Jakmile narazí na takovou adresu, tak ji prostě prohlásí za neexistující a spamoví roboti do nich už dále nerozesílají.

Po zkontrolování příchozích emailů na serveru, se emaily rozdělí do tři skupin. Zeleně se označí emaily od přátel a ty emaily, které se zdají asi legitimní. Červeně se pak označí ostatní emaily jako spamy. Spamové emaily pak můžeme velmi snadno odstranit a nestáhnou se nám do PC. Propustí se pak jen ty co spamem z největší pravděpodobností nejsou. Nevýhodou je, že funguje pouze na jeden emailový účet.

MailWasher se dá, ale taky pořídit jako PRO verze, za kterou se už, ale platí. Cena se pohybuje kolem 1000Kč. Verze PRO nabízí češtinu a tím pádem i snazší orientaci v programu.

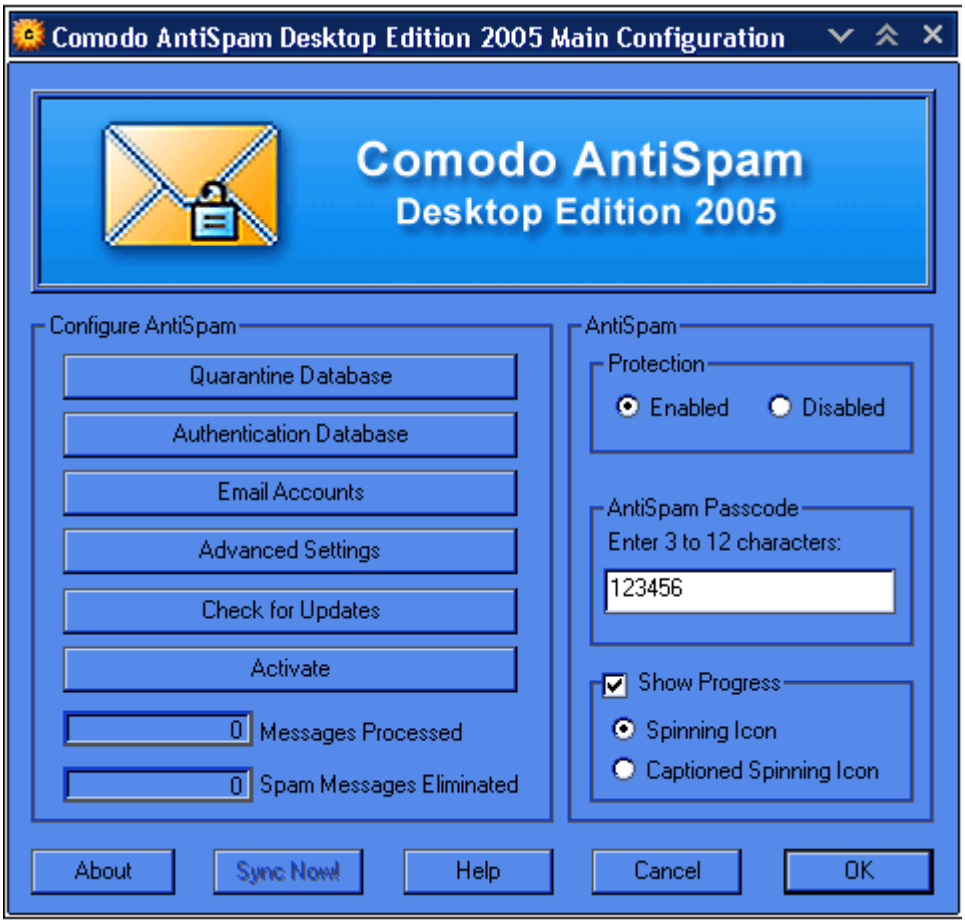


Obrázek 25: MailWasher [16]

5.2.2 Comodo AntiSpam Desktop 2005

Jakmile se program nainstaloval, tak byl vyžadován restart systému. S tím jsem se setkal poprvé. Program nebyl v češtině, tak jsem se potýkal s nastavením emailového klienta. Nastavení, ale nebylo moc obtížné, tak by to měl zvládnout i uživatel bez znalostí anglického jazyka. Program disponuje nastavení svých vlastních blacklistů a whitelistů. Je kompatibilní s aplikacemi jako Outlook, Outlook Express, Eudora, Netscape Messenger, a dalšími POP3 a SMTP emailovými účty a klienty. Filtry filtrují poštu do čtyř kategorií. Povolené, blokované, čekající na autentizaci a čekající na vymazání.

Uživatelské rozhraní:

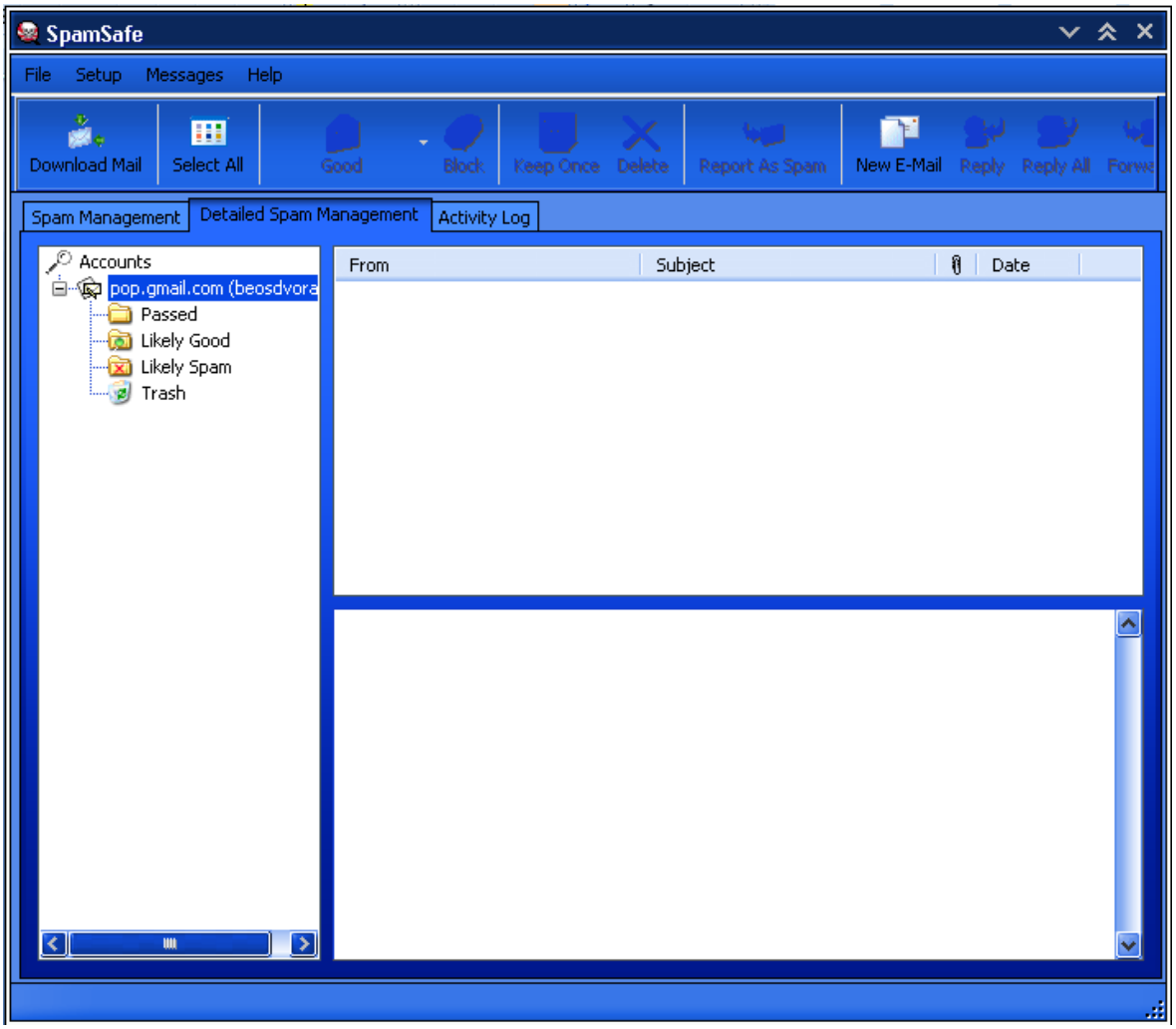


Obrázek 26: Comodo AntiSpam Desktop 2005

S tímto programem se mi vyskytl jeden problém a to s komunikačním programem jménem QIP. Bohužel jsem nepřišel na to jak tento problém odstranit a tak když je v PC nainstalovaný Comodo AntiSpam Desktop 2005, tak QIP prostě nepojede. Comodo ho nějak blokuje.

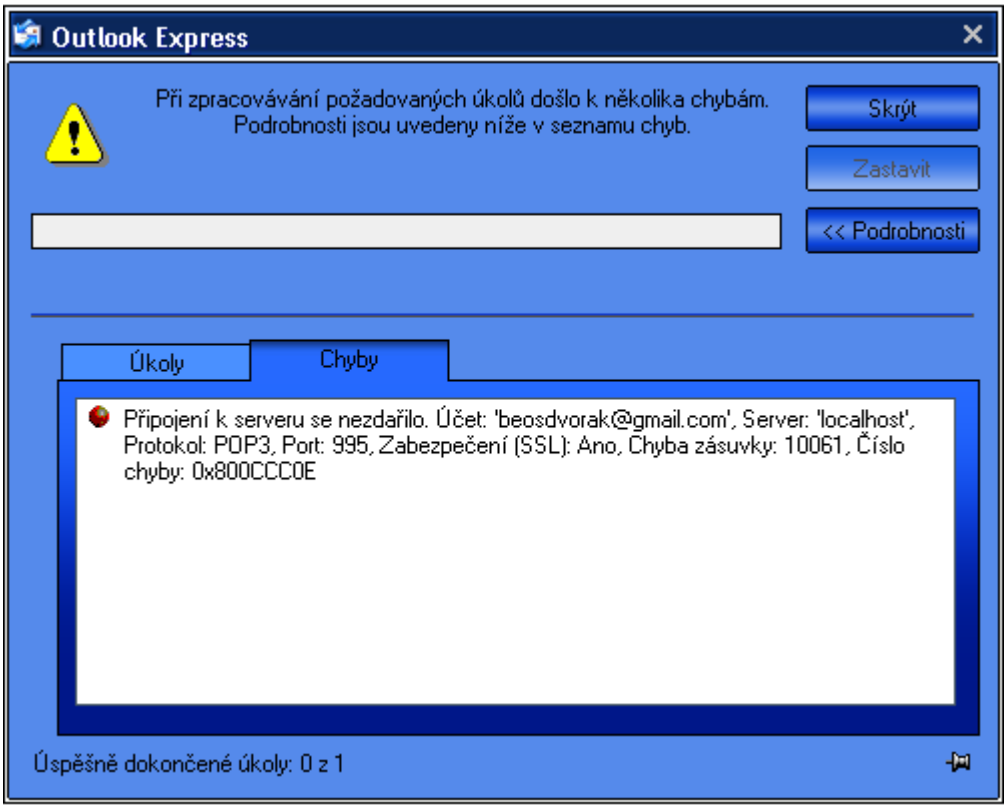
5.2.3 SpamSafe

Po nainstalování programu proběhne automatická aktualizace na nejnovější verzi. Program opět není v češtině a tak nastavení našeho emailového účtu musí proběhnout za pomocí slovníku nebo znalostí angličtiny. SpamSafe podporuje nejrůznější emaily. POP3, IMAP, AOL, MSN, HOTMAIL a YAHOO ve spolupráci s poštovními klienty jako je např. Outlook, Mozilla nebo Eudora. Program nabízí definováni vlastních blacklistů a whitelistů. SpamSafe poštu nejprve stáhne, což se liší od předchozího programu a je mnohem rizikovější. Pak poštu rozdělí do 4 složek. Na emaily, které jsou vyhodnoceny jako prošlé, pravděpodobně dobré, pravděpodobně spam a koš.



Obrázek 27: SpamSafe

Jenže hned po nainstalování se mi s mým poštovním klientem vyskytly potíže. Pokusil jsem se nastavit jako výchozí emailovou schránku Outlook Express. Po tomto nastavení jsem chtěl stáhnout poštu a Outlook mi oznámil nějakou chybu s POP3 serverem. Odstraněné této chyby mi zabralo dost času. Nemohl jsem přijít, o jakou chybu se přesně jedná, a tudíž jsem si nevěděl rady, jak daný problém vyřešit. V poštovním klientovy Outlook Express jsem zkoušel vše znova pře nastavovat, ale nic nepomohlo. I když jsem SpamSafe odinstalovat a vyčistil registry, dokonce i celý systém, tak to nepomohlo. Chyba pořád přetrvávala. Po dlouhém zkoušení všeho možného jsem nakonec přišel na to, jak problém vyřešit a chybu opravit. Pomohlo pouhé obnovení celého systému PC. Vrátil jsem výchozí nastavení systému zhruba o týden, což znamenalo, že SpamSafe ještě v té době nebyl instalován a chyba tím pádem nikdy nevznikla. Poštovní klient Outlook Express zase jel bez sebe menších problému jako dřív.



Obrázek 28: Chyba

SpamSafe mě teda vůbec nijak neoslovil, řekl bych, že je to průměrný až podprůměrný program na ochranu před nevyžádanou poštou. Navíc jsem s ním měl více problémů než užitku.

5.3 Program pro kompletní zabezpečení počítače

5.3.1 Kaspersky Internet Security

Kaspersky Internet Security je program pro kompletní ochranu počítače od tvůrců jednoho z nejlepších antivirů na světě. Chci otestovat, jestli takto komplexní program, který obsahuje i antispam, dokáže konkurovat programům, co byly přímo vytvořeny na ochranu před nevyžádanou poštou. Jde o placenou verzi, která poběží tři týdny zdarma. Program obsahuje antivirus, vlastní firewall, antispyware a antispam. Zaměřím se hlavně na antispam.

Antispam je obyčejný a základní, chybí tady definování blacklistů a whitelistů nebo filtrace pomocí rozpoznání cizích jazyků. Pošta je sice filtrována, ale jen v základním měřítku. Podporuje POP3, SMTP a IMAP a dokáže taky spolupracovat s klientem

Microsoft Office Outlook. Vše se nastavuje úplně samo a automaticky a není tady žádné širší nastavení. Jako kompletní řešení ochrany PC je, ale velmi dobrý a snadný na ovladatelnost. Chybí čeština, ale řekl bych, že tady ani není nutná. Nic se nemusí nastavovat a program automaticky zapne všechny ochrany od firewallu až po antispam a běží po celou dobu zapnutého PC, což přináší nepřetržitou ochranu. Databáze se také aktualizuje automaticky. Cena se pohybuje od 900Kč.

Obrázek 29: Kaspersky Internet Security

Kaspersky internet security by zasloužil mnohem hlubší analýzu, ale jelikož má práce pojednává hlavně o nevyžádané poště, tak jsem se převážně zaměřil jen na ni.

5.4 Srovnání produktů

Testoval jsem placený softwarový program, neplacené (freewarové), a program pro kompletní internetovou ochranu, který obsahoval i mimo jiné antispam. Musím říct, že s placeným softwarem jsem byl opravdu spokojený. Všechno bylo v češtině a velmi jednoduché. Nemusel jsem skoro nic nastavovat, program si vše udělal sám. Spojil se svým

serverem, aby mohl filtrovat spam emaily. Obsahoval definování vlastních blacklistů a whitelistů a navíc filtraci podle rozpoznáním cizího jazyka, což mě velmi zaujalo. Tento program byl na velké profesionální úrovni.

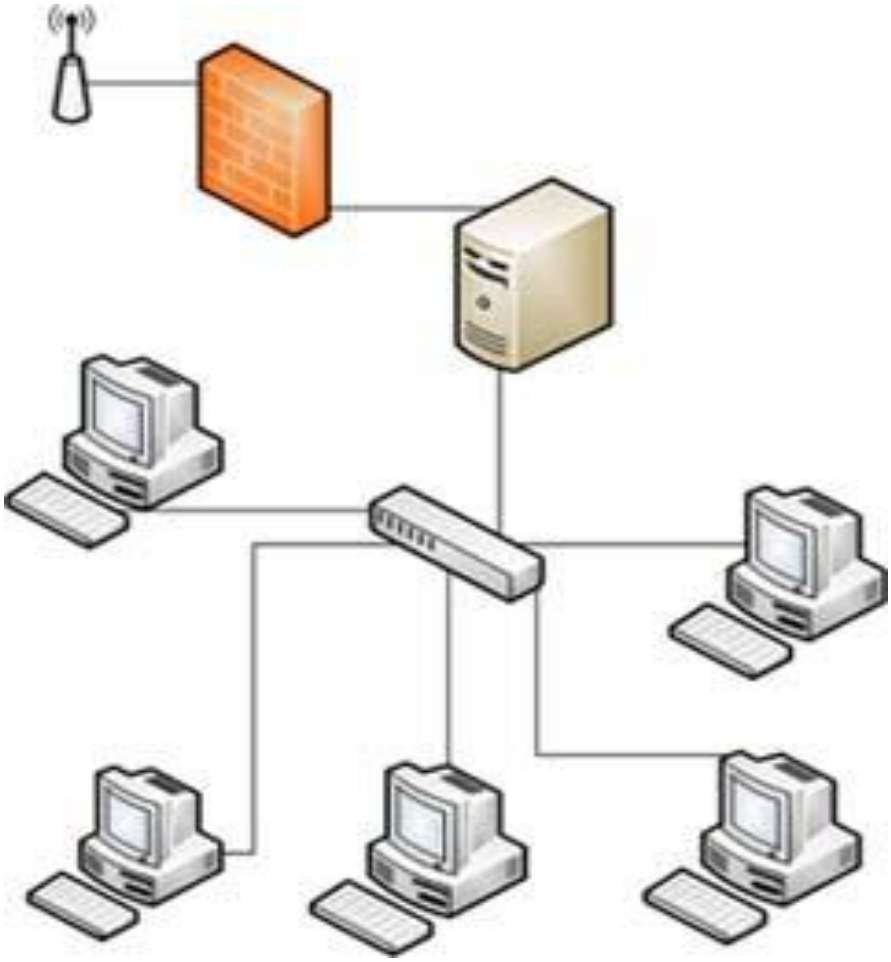
Neplacené softwarové verze mě už tak neoslovily. U všech jsem postrádal češtinu. Vše se nastavovalo ručně, což bylo hodně složité a zabíralo to více času. Navíc jsem se potýkal z pár problémy. Program Comodo AntiSpam Desktop 2005 mi zcela blokoval komunikační program QIP. Nepřišel jsem na to, čím to mohlo být způsobené. Další problém, který se ale vyskytl v mém poštovním klientovi Outlook Express, byla chyba, která mi zcela zablokovala stahování pošty. Tento problém nastal po nainstalování programu SpamSafe. Odstranění tohoto problému my zabralo spoustu úsilí a času. Nakonec se mi, ale problém podařilo úspěšně vyřešit a odstranit a mohl jsem pokračovat v testování.

Posledním programem byl Kaspersky Internet Security na kompletní ochranu PC. Tento program se mi taky dost líbil a byl také na velmi profesionální úrovni. Byla to placená verze, která běžela tři týdny zdarma. Nebyla sice v češtině, ale myslím si, že čeština tady není vůbec potřeba, protože program vše dělat úplně sám a automaticky. Nebylo zapotřebí nic nastavovat. Ochrana před nevyžádanou poštou byla průměrná, filtr sice blokoval, co se dalo, ale chybí tady nějaké širší nastavení a rozvinutí. Když se ale skloubí tolik věci do jednoho programu, tak se není co divit. Doporučoval bych tento program kombinovat s nějakou z placených verzí antispamových programů např. SPAMfighter a ochrana našeho PC by byla na velmi vysoké úrovni. Řekl bych, že dosáhnout vyšší ochranné úrovně by se snad ani už dosáhnout nedalo.

Placené verze převyšovaly skoro ve všech věcech ty neplacené. Jednoduchost, ovladatelnost, stupeň ochrany, orientace v programu, zabezpečení, takže jsem zcela pro placené verze. Ceny nejsou nějak vysoké a odpovídají tomu, co za ni dostaneme. Na neplacených verzích se dá sice ušetřit, ale problémy jaké se mi vyskytly, za to nestojí. Asi jediný freewarový program, který je celkem na slušné úrovni, byl SpamWasher. S tím jsem byl taky hodně spokojený. Doporučoval bych, ale placený software, opravdu nestojí tolik a tato investice se určitě vyplatí.

6 OCHRANA FIREMNÍ SÍTĚ

V dnešním globálním internetovém věku, je ochrana firemních dat a zabezpečení před hrozbami z internetu na prvním místě v každé firmě. Důvod je prostý. Jakýkoliv výpadek, napadení z internetu, či útok ze vnitř sítě může citelně ochromit chod firmy. Nejedná se už jen o pouhé hrozby, jako jsou počítačové viry, poruchy hardwaru a jiné nezávislé poruchy. V ostrém konkurenčním boji jsou taseny zbraně mnohem ostřejšího kalibru, jako cílené průniky do firemních sítí, krádeže firemních nebo důvěrných dat, odposlechy emailové komunikace, nebo útoky pomocí sociálního inženýrství. V poslední době to, ale bývají převážně spamy, které zcela ochromují firemní sítě. Nevyžádanou poštou totiž může přijít velké množství aspektů, od těch méně nebezpečných jako jsou reklamy, až po nebezpečné jakou jsou viry nebo phishing. V následujících scénářích se budu zabývat zabezpečení firemní sítě, které rozložím do tří bodů. Budu se věnovat jenom zabezpečením proti nevyžádané poště, protože o tom pojednává moje práce.



Obrázek 30: Příklad firemní sítě [17]

6.1 Zabezpečení firemních serverů

První metoda jak zabezpečit firemní síť je zabezpečit firemní servery. Podle velikosti firemní sítě může mít firma jeden nebo více serverů, které tuto firemní síť budou spravovat. Dejme tomu, že máme firmu, která má okolo 2000 počítačů. Zabezpečit takto rozsáhlou firemní síť není nic jednoduchého. Jediné východisko, které se nám nabízí je zabezpečit firemní server. Tato síť může mít více serverů a my se budeme zabývat mail serverem, který bude spravovat veškerou poštu určenou z do firemní sítě. Je mnohem lepší zabezpečit mail server, než všechny ostatní osobní firemní počítače, protože to ušetří mnohem více peněz, než kdybychom instalovaly na každý počítač nějaký antispamový program zvlášť. Navíc při tak hojném počtu by se nemuselo uhlídat, jestli si každý zaměstnanec pravidelně aktualizuje svůj antispam a stará se o něj. Z pravidla když člověk něco nevlastní nebo není jeho, tak se moc nestará o to, co by se mohlo stát a tady by následky pro firmu mohly být velmi velké. Sice zase musíme mít velkou kapacitu mail serveru, protože bude spravovat velké množství emailů. Tato možnost je opravdu mnohem efektivnější a levnější. Server bude od nevyžádané pošty spravovat firemní emaily. Na firemní server bych nainstaloval nějakou verzi placeného softwaru, aby byla ochrana před nevyžádanou poštou na co nejvyšší úrovni. Server z internetu příjme poštu, kterou následně vyhodnotí podle svých filtrů, nebo podle předem definovaných blacklistů. Rozhodně bych také nadefinoval whitelisty. Dal bych tam adresy, které firma často používá a nehrozí od nich žádny útok ve formě spamů. Podle stanovených kritérii server vyhodnotí, zda jde o spam, podezřelou poštu nebo o poštu, která nenese žádné rizika. Následně pak bezpečnou poštu propustí k osobním firemním počítačům a spam zachytí. Spam pak vymaže. Některé programy taky nabízí, že nevyžádanou poštu vrátí autorovy v takovém formátu, že to vypadá jako by tato emailová adresa vůbec neexistovala. Takto by firemní emaily měli být relativně dobře zabezpečené. Přes emaily by se teda neměly dostat žádné viry, nebo phisingové zprávy, které by mohli vést ke krádeži dat nebo sabotáži a dalších pro firmu nebezpečných věcí.

Firemní politika by měla zakazovat používat zaměstnancům freemailové účty. Vysvětlení je následující. Firemní email bude zcela bezpečný, tak nehrozí žádné nebezpečí. Jakmile ale nějaký zaměstnanec bude hojně používat svůj vlastní freemailový účet a to takovým způsobem, že nebude dbát na jakoukoliv bezpečnost, což znamená, že nejen otevře, ale bude i reagovat na emaily nebezpečného charakteru, tak velmi ohrozí celou firemní síť. Jakmile otevře spamový zavirovaný email, který v okamžiku infikuje jeho firemní počítač

nějakým červem nebo virem, může to mít katastrofální následky pro celou firemní síť. Vir nebo červ se muže po firemní síti rozšířit do všech počítačů velmi rychle a než si někdo něco uvědomí, bude infikována celá firemní síť.

6.2 Zabezpečení osobních počítačů firmy

Tento návrh bych realizoval v nějaké malé firmě, která skýtá pouze desítky osobních firemních počítačů. Jak jsem psal výše, tak při více počítačích by bezpečnost nemusela být uhlídána. V takové malé firmě by byl jen jeden server, který by mohl mít malou kapacitu, a tím pádem by se do něj nemuselo tolik investovat. Ušetřením peněz na serveru by se nakoupily antispamové softwary do jednotlivých osobních firemních PC. Samozřejmě by tento server nemohl být úplně bez žádného programu. Stačil by nějaký slušný firewall, aby nepropouštěl nežádoucí pakety. Pro osobní firemní PC bych navrhoval takový antispamový program, který umí filtrovat poštu přímo na serveru, to znamená, že ještě než stáhneme poštu do PC, tak ji server zachytí, přefiltruje a pak ji propustí. Navíc nadefinováním blacklistů a whitelistů usnadníme programu rychlejší kontrolu zpráv. Jakmile by se totiž na server dostlala pošta od zdroje, který je na blacklistu nebo whitelistu, tak program by ji okamžitě vymazal nebo propustil na náš osobní firemní počítač.

V takovémto případě by se dalo umožnit používat osobní freemailové účty. Program by totiž na každém z osobních PC filtroval poštu a zabraňoval tak průchodu nevyžádané pošty. Musel by to ale být takový program, který umožňuje chránit více emailových účtů.

6.3 Kombinované zabezpečení

Kombinovaným zabezpečením myslím to, že se zabezpečí placeným softwarem jak firemní mail server, tak i osobní počítače. Je to nejefektivnější způsob zabezpečení a, řekl bych, že poskytuje nejvyšší stupeň zabezpečení. Musíme se ale zamyslet nad tím, do jak velké firmy bychom tento způsob zabezpečení chtěly realizovat. Kdyby se jednalo a malou až středně velnou firmu, která neskýtá velké množství osobních firemních PC, tak by náklady nemusely být až tak velké. A tato realizace zabezpečení by se určitě vyplatila. Měli bychom na mail serveru kvalitní antispamový program, který by filtroval poštu firemním mailům a zároveň by na každém osobním PC byl také nainstalovaný antispam. Tento antispam by pomáhal mail serveru, aby nebyl tak zatěžován. Při takovémto stylu zabezpečení by firemní politika mohla povolovat používání freemailových účtů na

osobních počítačích. Antispam by se postaral o filtraci těchto účtů, protože by byl na každé osobní stanici.

Kdybychom toto zabezpečení chtěli realizovat v nějaké hodně velké firmě, tak náklady na pořízení antispamu do všech osobních firemních počítačů by rapidně vzrostly. A zase uhlídat, aby všichni pravidelně aktualizovali a chovali se v emailových účtech aspoň podle nějakých bezpečnostních pravidel, by nebylo jednoduché.

Při této realizaci by teda záleželo na peněžních prostředcích firmy a taky hlavně na velikosti firmy (počtu osobních firemních počítačů).

ZÁVĚR

V úvodu práce popisuji jeden z největších fenoménů poslední doby a to je spam neboli nevyžádaná pošta. V teoretické části se zaměřuji na druhy spamů a jeho formy. Vysvětluji jak se spam šíří, jaké jsou nejpoužívanější metody šíření a kde se nejvíce se spamem setkáváme. Popisuji proč je spam tak nebezpečný a jaké konkrétní rizika nám hrozí. V nevyžádané poště totiž mohou být tak zákeřné viry, které nám zcela mohou zablokovat systém nebo ukrást naší identitu, popřípadě vykrást náš bankovní účet během chvilky. Hlavně se ale zaměřuji na to, jaké máme metody obrany proti nevyžádané poště. Podrobně rozepisuji nejčastější a nejpoužívanější metody ochrany před spamem.

Praktická část pro mě byla opravdovou výzvou. Testoval jsem nejrůznější antispamové programy. Rozdělil jsem je na placené a neplacené verze. Při testování placené verze antispamové programu jsem byl mile překvapen jak všechno plynule a bez potíží běželo. Program, který jsem testoval, byl na velké profesionální úrovni a měl velký stupeň zabezpečení. Mohu jen doporučit. S freewarovými verzemi programů jsem už tak spokojený nebyl. Vyskytly se některé potíže, které mi zcela ochromily mou emailovou schránku v Outlook Expressu. Po nainstalování jednoho programu mi zcela můj klient přestal fungovat. Vyskytla se chyba a odstranění této chyby mi zabralo dost času. Nemohl jsem přijít proč a hlavně jak tuto chybu odstranit. Nakonec se mi to ale úspěšně povedlo a můj klient už běží bez problémů a testování dalších programů mohlo pokračovat.

Nakonec jsem navrhl zabezpečení firemní sítě proti spamu. Nastínil jsem tři scénáře pro tři různé typy zabezpečení.

Myslím si, že jsem splnil vše, co bylo v zadání této práce.

CONCLUSION

In the introduction, thesis describes one of the largest recent phenomena and it is spam or unsolicited email. The theoretical part focuses on the types and forms of spam. Explain how to spread spam, what are the most common methods of diversion and where most spam is encountered. It describes why spam is so dangerous and what the specific risks we are threatened. In the spam can be so insidious viruses, we can completely block the system or steal our identity and, where appropriate, rob our bank account within a minute. Mainly, however, focuses on what we have methods of defense against spam. Describes in detail the most common and most methods of protection against spam.
Practical part for me was a real challenge. I tested a variety of antispam programs. I divided the paid and unpaid versions. When testing paid version of the antispam program, I was pleasantly surprised how smoothly everything ran without problems. The program, which I tested, was the major professional level and have a high degree of security. I can only recommend. With a freeware version of the program I was already unsatisfied. There were some problems that I completely crippled my email account in Outlook Express. After you install a program I completely stopped my client work. An error occurred and the elimination of this error I took enough time. I could not come and why especially as this error. Finally, I succeeded but successful and my client is already running smoothly, and testing other programs to continue.
Finally, I designed corporate network security against spam. I outlined three scenarios for three different types of security.
I think that I have fulfilled everything that was in the award of this work.

SEZNAM POUŽITÉ LITERATURY

[A] ADÁMEK, Martin. *Spam : Jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu*. Praha : Praga, 2009. 168 s. ISBN 978-80-247-2638-0.

[B] POLČÁK, Radim. *Právo na internetu : Spam a odpovědnost ISP*. Brno : Computer Press, 2007. V,150 s. ISBN 978-80-251-1777-4.

[1] Wikimedia Foundation, Inc.. *Wikipedie, otevřená encyklopedie : Spam* [online]. 2009 [cit. 2009-03-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Spam>.

[2] *Flickr* [online]. 2009 [cit. 2009-03-05]. Dostupný z WWW: <http://www.flickr.com/photos/garaolaza/2894611244/>.

[3] *Fortinet* [online]. 2009 [cit. 2009-03-05]. Dostupný z WWW: <http://kc.forticare.com/admin/virtual/imgs/outlook-spam-2.jpg>.

[4] *LUPA : Obrázkový spam* [online]. 2006 [cit. 2009-03-06]. Dostupný z WWW: <http://pavel.blog.lupa.cz/2006/08/01/obrazkovy-spam/>. ISSN 1213-0702.

[5] NYKODÝMOVÁ, Helena. *LUPA* [online]. 22. 5. 2007 [cit. 2009-03-07]. Dostupný z WWW: <http://www.lupa.cz/clanky/spam-nabira-na-sile-zlocinci-se-organizuji/>. ISSN 1213-0702.

[6] *Sophos* [online]. 1997-2009 [cit. 2009-03-10]. Dostupný z WWW: <http://www.sophos.com/pressoffice/news/articles/2007/04/dirtydozapr07.html>.

[7] Wikimedia Foundation, Inc.. *Wikipedie, otevřená encyklopedie : Simple Mail Transfer Protocol* [online]. 2009 [cit. 2009-03-11]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol>.

[8] PALEČEK, Lukáš. *AudiV8* [online]. 2006-2009 [cit. 2009-03-14]. Dostupný z WWW: <http://www.audiv8.cz/clanky_read.php?clanek-nazev=Spam-a-antispamova-ochrana&id=19&rubrika=2>.

[9] KRYL, Milan. *Milan Kryl web : Spam - nevyžádaná pošta* [online]. 30. 6. 2004 [cit. 2009-03-16]. Dostupný z WWW: <http://kryl.info/spam.html>.

[10] KŘIHOHLÁVEK, Jindřich. *EMAG* [online]. 13. února 2008 [cit. 2009-03-20]. Dostupný z WWW: <http://www.emag.cz/vy-jeste-nemate-gmail/>. ISSN 1802-4238.

[11] DOČEKAL, Daniel. *POOH* [online]. 3.12.2001 [cit. 2009-03-28]. Dostupný z WWW: <http://www.pooh.cz/pooh/a.asp?a=2003842&db=1001>.

[12] MIKULA, Jan. *Prohlížeče* [online]. 2005-2009 [cit. 2009-04-05]. Dostupný z WWW: <http://prohlizece.info/clanky/bezpecnost-internetoveho-bankovnictvi-phishing-aneb-jak-napalit-klienta-3-dil/>. ISSN 1802-3584.

[13] *BusinessWeek : Bayesovká logika a dnešní vypočitatelný svět.* [online]. Květen 24, 2005 [cit. 2009-04-29]. Dostupný z WWW: <http://www.businessweek.cz/bayesovske-filtry-logika-spam.html>.

[14] *Softpedia : Anti-Spam Blacklist Thing Screenshots* [online]. 2001-2009 [cit. 2009-05-10]. Dostupný z WWW: <http://www.softpedia.com/progScreenshots/Anti-Spam-Blacklist-Thing-Screenshot-62248.html>.

[15] *Advanced Searchbar* [online]. 2007 [cit. 2009-05-10]. Dostupný z WWW: <http://iebrowsertuner.com/features.htm>.

[16] Firetrust Ltd. *MailWasher* [online]. [2008] [cit. 2009-05-12]. Dostupný z WWW: <http://www.mailwasher.net/>.

[17] *I-SERVICES : Návrh a správa firemních sítí* [online]. [2008] [cit. 2009-05-12]. Dostupný z WWW: <http://www.i-services.cz/navrh-a-sprava-firemnich-siti.p5.html>.

[18] ZACHR, Václav. *Elektronická pošta : SMTP protokol* [online]. [2006] [cit. 2009-05-12]. Dostupný z WWW: <http://www.fi.muni.cz/~kas/p090/referaty/2006-podzim/ct/xzachr-smtp.html#smtp>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AOL America Online - je to poskytovatel internetových služeb, náležící k mediálnímu koncernu Time Warner.

DOS Denial of service - Jsou to takové útoky, které jsou namířeny proti serverům nebo proti celým sítím.

ICQ I Seek You, - je software pro instant messaging využívající protokolu OSCAR.

IMAP4 Internet Message Access Protocol version 4 - je internetový protokol pro vzdálený přístup k e-mailové schránce.

IP Internet Protokol - je datový protokol používaný pro přenos dat přes paketové sítě.

MDA Mail Delivery Agent - program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.)

MSN Microsoft Network - je kolekce internetových služeb společnosti Microsoft

MTA Mail Transfer Agent - server, který se stará o doručování zprávy na cílový systém adresáta

MUA Mail User Agent - poštovní klient, který zpracovává zprávy u uživatele

P2P Peer to peer - označují se tak počítačové sítě, ve kterých spolu komunikují přémo jednotlivý klienti

POP3 Post Office Protocol version 3 - je to internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta.

QIP Quiet Internet Pager - je počítačový program pro rychlé zasílání zpráv (tzv. instant messaging) založené především na protokolu OSCAR.

RFC request for comments - používají se pro označení řady standardů a dalších dokumentů popisujících Internetové protokoly, systémy apod.

SMTP Simple Mail Transfer Protocol - je internetový protokol, který se pužívá pro přenos zpráv elektronické pošty

SW software - je v informatice sada všech počítačových programů v počítači

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: KOMUNIKACE SMTP

S: 220 bubo.vslib.cz 5.67a8/IDA-1.5 Sendmail is ready at Mon,
28 Feb 1994 14:34:59 +0100
C: HELO ns.felk.cvut.cz
S: 250 Hello ns.felk.cvut.cz, pleased to meet you
C: MAIL From:<csTeX-Mgr@cs.felk.cvut.cz>
S: 250 <csTeX-Mgr@cs.felk.cvut.cz>... Sender ok
C: RCPT To:<MILAN.KERSLAGER@VSLIB.CZ>
S: 250 <MILAN.KERSLAGER@VSLIB.CZ>... Recipient ok
C: RCPT To:<VIT.ROCEK@VSLIB.CZ>
S: 250 <VIT.ROCEK@VSLIB.CZ>... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Received: from mvax.felk.cvut.cz by ns.felk.cvut.cz
(5.65c8/FELK-area.4.2)
C: id AA00728; Mon, 28 Feb 1994 14:31:46 +0100
C: Message-Id: <199402281331.AA00728@ns.felk.cvut.cz>
C: X-Listname: Czech and Slovak TeX-related mailing list
<csTeX@cs.felk.cvut.cz>
C: Warnings-To: <>
C: Errors-To: csTeX-Mgr@cs.felk.cvut.cz
C: Sender: csTeX-Mgr@cs.felk.cvut.cz
C: Received: by cs.felk.cvut.cz (MX V3.3 VAX) with SITE;
Mon, 28 Feb 1994 14:21:52
C: MET-2DST
C: Date: Mon, 28 Feb 94 14:21:23 MET
C: From: HORAKK%CSEARN.BITNET@earn.cvut.cz
C: Reply-To: csTeX@cs.felk.cvut.cz
C: Subject: Re: inspic lde 3/92
C: To: csTeX@cs.felk.cvut.cz
C:
C: Mohu Vam zminene makro poslat mailem.
C:
C: Karel Horak
C: .
S: 250 Ok
C: QUIT
S: 221 bubo.vslib.cz closing connection

Pro úplnost ještě uvedu další příkazy, které SMTP definuje:

- VRFY – ověření adresy
- EXPN – rozvinutí aliasů adresy
- NOOP – prázdný příkaz
- RSET – zrušení zasílání dopisů (místo RCPT To: nebo DATA)
- HELP – vypíše seznam příkazů“ [18]