Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava 4

Moderné hrozby malware-u

Roman Panenka

Študijný program: Počítačové komunikačné systémy a siete

Ročník: Ing. 1

Predmet: Bezpečnosť počítačových systémov

Ak. rok: 2010/11

Obsah

1. Stručný prehľad problematiky

Slová ako spyware, vírus, červ... sa často krát používajú na opis všetkých súčasných kyber hrozieb. Pritom tieto slová sú len malá časť veľkej rodiny škodlivého kódu a taktík pod menom Malware.

Malware je všeobecné označenie pre škodlivý kód. Najčastejšie to môže byť počítačový vírus, červ alebo stále Trojský kôň. Všeobecne je nazývané ako nechcený alebo nežiaduci softvér a je majoritným problémom súčasného prostredia IKT. S príchodom a veľkým rozmachom webových technológií sa začali šíriť desiatky nových tipov malwaru, jeden prefíkanejší ako druhý. Kedysi sa malware šíril hlavne na vymeniteľných médiách alebo prostredníctvom e-mailových správ.

V súčasnosti existuje obrovské množstvo taktík a spôsobov útoku malwaru. Krásnou ukážkou je sociálne inžinierstvo, kedy vám v správe príde odkaz na škodlivý kód pod zámienkou, že odkaz smeruje na zaujímavý obrázok alebo video. Keď neopatrný a nezabezpečený používateľ na odkaz klikne, stiahne si namiesto sľubovaných obrázkov škodlivý kód. Navyše šikovný malware daný obrázok aj zobrazí aby si používateľ nič nevšimol.

Brániť sa voči moderným spôsobom malwaru nie je ľahké. Avšak pri použití kvalitného anti-malware programu, aktualizovaného operačného systému a programov tretích strán a hlavne s použitím zdravého rozumu sa dajú riziká to veľkej miery obmedziť. Treba však dodať, že tvorcovia malwaru sú vždy krok pred výrobcami anti-malware-u, a preto treba byť obozretný.

Vo svojej práci sa preto budem snažiť predostrieť klasické a hlavne moderné typy škodlivého kódu. Veľká časť moderného malwaru sa sústreďuje hlavne na najrýchlejšie sa rozvíjajúci IT platformu - webovú platformu a internet. Malware nie je už zábavka unudených programátorov a neprajníkom, ale aktuálna hrozba v oblasti financií, informácií, všetkých smerov bezpečnosti. V podstate sa pri vhodnom nasadení dotýka všetkých hlavných pilierov modernej spoločnosti.

1.1.Zoznam vybratých otázok

Vo svojej práci sa budem orientovať na zodpovedanie a vyjasnenie nasledujúcich otázok. Otázky sa týkajú problematiky aktuálnych malware hrozieb, nasadzovania protiopatrení proti týmto hrozbám a ďalších načrtnutých v sekcií Stručný prehľad problematiky.

- Čo je to malware a aké typy malwaru sú rozšírené
- Je pre nás malware hrozbou?
- V ktorých oblastiach sveta sa malware najviac sústreďuje?
- Je súčasný informačný priestor bezpečnejší vďaka pokročilejším technikám detekcie škodlivého kódu ?
- Aké sú moderné typy malwaru?
- Ktoré rodiny malwaru nám predstavujú v súčasnosti najväčšiu hrozbu?
- Ako sa bojuje proti modernému malwaru?

2. Čo je to malware

„Malware“ sú malé počítačové programy alebo ich časti, ktoré majú škodlivý alebo zlomyseľný (malicious » mal » malware)vplyv na bezpečnosť počítača používateľa. Malware sa do počítača v dnešnej dobe dostane najčastejšie prostredníctvom internetu. Táto pravdepodobnosť sa zvyšuje hlavne slabou ochranou koncového počítača a navštevovaním škodlivých stránok.

Malware pokrýva mnoho známych pojmov ako vírus, trojský kôň, červ alebo menej známych ako rootkit, spyware a pod. V prvej časti tejto práce si rozoberieme a definujeme hlavné vlastnosti najznámejších typov malwaru. Nasledujúca kategorizácia je len jednou z mnohých používaných a často sa stáva, že jeden záškodný program môže patriť do viacerých typov malwaru naraz.

2.1.Vírus

Počítačový vírus je program, ktorý je schopný vytvoriť svoju funkčnú kópiu a následne ju aktivovať. K základným vlastnostiam vírusov patrí tiež ich schopnosť rozmnožovať sa. Podmienkou existencie a množenia vírusov je existencia vírusového hostiteľa, v ktorom majú vhodné podmienky existencie.

Cieľom infekcie je najčastejšie iný program, boot sektor pevného disku alebo rozličné dokumenty. Najbežnejší spôsob rozmnožovania je pripojenie svojej kópie na koniec programu alebo do vnútra dokumentu. Vírus môže vykonávať nebezpečnú činnosť v počítači bez vedomosti používateľa. Okrem rozmnožovania má aj ďalšie škodlivé účinky, ako napr. modifikácia alebo zničenie údajov v súboroch, deštrukcia údajov pevného disku, spomalenie činnosti počítača.

2.2.Červ

Červ je typ vírusu ktorý sa šíri pomocou e-mailov alebo intranetovej siete. Na rozdiel od klasických súborových vírusov sa väčšina červov nereprodukuje v takom veľkom množstve, veľká časť sa dokonca nereprodukuje vôbec a na infiltrácie využíva pôvodnú vzorku. Dôsledkom rozšírenosti internetu je červ schopný rozdistribuovať sa po celom svete v priebehu niekoľkých hodín. Vedľajším efektom môže byť kompletné zahltenie siete, nevnímajúc podnikové LAN.

Elektronickou poštou zasiela emaily osobám obsiahnutým v knihe kontaktov alebo odosiela svoje kópie aj na adresy vyskytujúce sa v emailoch používateľa. Takýmto spôsobom môže používateľovi prísť email od neznámeho človeka obsahujúci červa a preddefinovaný text z tela vírusu alebo s textom, ktorý obsahoval ľubovoľný email v schránke odosielateľa. čím červy veľkou mierou zasahujú do súkromia používateľa

2.3.Trójsky kôň

Je to škodlivý program, ktorý nemá schopnosť samostatne sa kopírovať a infikovať súbory, tak ako to dokážu vírusy alebo červy. Najčastejšie sa vyskytuje ako spustiteľný súbor. Trójsky kôň sa vyskytuje na počítači spravidla iba v jednom exemplári, ktorý neobsahuje nič iné ako telo spomínanej infiltrácie. Vykonáva deštruktívnu činnosť, pričom sa vydáva za užitočný program. Tento typ infiltrácie má rozličné funkcie, od zasielania stlačených kláves (keylogger) až po mazanie súborov (sformátovanie disku).

Zvláštnou funkciou je inštalovanie tzv. backdooru. Najúčinnejší spôsob odstránenia tohto nevyžiadaného programu je veľmi jednoduchý a to jeho zmazanie.

2.4.Backdoor

Backdoor, alebo „zadné dvierka“ je aplikácia, ktorá umožní autorovi vzdialený prístup na počítač. Na internete existujú rôzne aplikácie, ktoré umožňujú používateľovi vzdialenú správu svojho počítača. Ak sa takéto aplikácie zneužijú, jeho vlastník netuší, že útočník má prístup k dátam a môže využívať tento počítač na posielanie spamu, alebo aj na rôzne hromadné útoky.

2.5.Rootkit

Rootkit je typ infiltrácie, ktorého účelom je zamaskovať bežiace procesy, súbory alebo iné údaje pred operačným systémom. Rootkit bol pôvodne určený na nedeštruktívne účely, ale v poslednej dobe sú stále viac a viac využívané rôznymi druhmi škodlivých kódov - malware. Pri rootkitoch je najdôležitejšia prevencia, čiže je nutné zabrániť infiltrácii skôr ako sa stihne rootkit aktivizovať. Rootkit sa dokáže v systéme po svojej aktivácii „zneviditeľniť“ a napadnutý užívateľ tak môže získať falošný pocit bezpečia.

3. Moderné typy malware-u

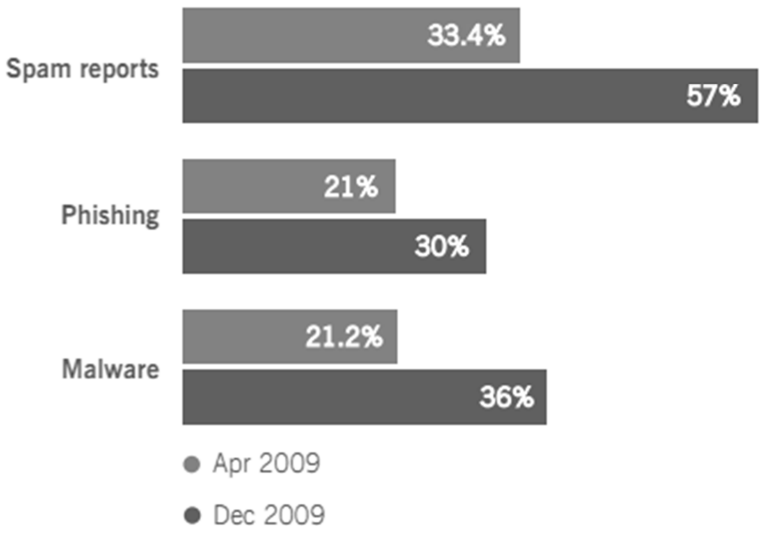
3.1. Badvertising a Adsploit

Najväčšia časť škodlivého kódu pochádzajúceho z internetu sa skrýva za reklamami. Tie na nás číhajú na každej stránke. Ponúkajú nám výhodne zľavy na množstvo produktov, reklamujú nám nové druhy výrobkov na trhu, často krát aj skutočné. Po kliknutí na takéto reklamy sa používateľovi síce zobrazí obsah, ktorý očakával (web stránka produktu) no medzitým sa stihol vykonať škodlivý kód. Často krát sa týmto spôsobom aj reklamujú podozrivé softvérové produkty, s ktorými získa útočník vzdialený prístup k počítaču používateľa.

Podobným druhom podvrhnutej reklamy sú malware typu Adsploit, ktoré menia texty známych internetových reklamných systémov, ako napr. Google AdSense

3.2. Anti social networking

Sociálne siete sa stali internetovým fenoménom posledných rokov. Sociálne siete navštevujú denne milióny ľudí a stále sa ich obľúbenosť zvyšuje. Nie je sa čo čudovať, že tieto stránky prilákali aj záškodnícky softvér. Sociálne siete ako Facebook, Twitter, MySpace, Orkut a pod. sa stali súčasťou bežného života ľudí a biznisu. Prihlasovacie informácie na tieto siete sa stali rovnako citlivými ako heslá na emailové účty, ak nie viac. Na obrázku



Obrázok 1 - nárast obľuby malware-u na sociálnych sieťach v minulom roku [1]

Koobface

Je sofistikovaný malware, ktorý sa orientuje na najväčšiu sociálnu sieť Facebook (z čoho má aj odvodený názov), no rozšíril sa aj na siete MySpace, hi5, Bebo, Friendster a Twitter. Dokáže vytvárať na sociálnej sieti vlastné účty a prostredníctvom nich posielať reálnym používateľom odkazy na podozrivé stránky s podvrhnutým malware-om alebo sebou samým. Koobface si dokáže tieto nové účty sám aktivovať, naplniť informáciami, pridať sa do náhodných skupín a nadviazať priateľstvo s rôznymi používateľmi.

Hlavným cieľom Koobface-u je infikovať reálne účty používateľov a následnej rozposielať správy s nebezpečnými odkazmi priateľom infikovaného používateľa. Keďže cieľový používateľ dôveruje správam od svojich kamarátov, klikne na odkaz a stane sa ďalšou obeťou Koobface-u. Následne sa proces opakuje s priateľmi novej obete. Snaží sa zozbierať čo najviac prístupových informácii na FTP účty, mailové účty a účty sociálnych sietí, no neorientuje sa na zber citlivých finančných informácií.

Clickjacking

Clickjacking je spôsob útoku na používateľov webových stránok (nie len sociálnych sietí), pri ktorom spustí na zdanlivo neškodnej stránke akciu, ktorú nepredpokladal. Táto technika využíva zraniteľnosť, ktorá sa vyskytuje vo väčšine prehliadačoch.

Stránka využívajúca clickjacking má na pozadí neškodný obsah – napr. fotogalériu a vedľa každej fotky odkaz, ktorý vedie na ďalší obrázok v poradí. Zároveň je však nad týmto odkazom ďalší odkaz na úplne inú stránku, ktorý ma ale nastavenú priehľadnosť, a tak ho používateľ nevidí. Keď sa následne používateľ pokúsi zobraziť ďalší obrázok, v skutočnosti klikne na podvrhnutý odkaz, ktorý ho dovedie na podvodnú stránku a tá mu upraví nejaké nastavenia.

Obeťou clickjackingu sa stávajú v posledných rokoch vo veľkej miere sociálne siete. Medzi prvé pokusy na facebooku patrilo generovanie fiktívnych chybových upozornení, čo nútilo používateľom klikať na tlačítka pre zavretie týchto okien. Medzi ďalšie pokusy sa ráta podvrhovanie skrytých odkazov k známym „Like“ facebook tlačítkam alebo používanie napínavých príbehov a atraktívnych dám na nalákanie nových obetí.

3.3.Phishing a odvodené metódy

Phising označuje činnosť, pri ktorej sa podvodník snaží vylákať od používateľov rôzne heslá, napr. k bankovému účtu. Väčšinou prebieha tak, že sa založí webstránka, ktorá vyzerá ako presná kópia už existujúcej dôveryhodnej stránky a na ktorej sú zachytávané prihlasovacie údaje obete. Môže prebiehať i tak, že sa rozposielajú e-maily, ktoré oznamujú používateľom zmenu účtu a tak lákajú heslá.

Pharming je zdokonalená metóda phishing-u ktorá presmeruje internetové spojenie medzi IP adresou a cieľovým serverom. K tomuto môže dôjsť na DNS serveri alebo prostredníctvom sociálneho inžinierstva alebo na lokálnom počítači prostredníctvom „Trójskeho koňa“ ktorý modifikuje príslušné súbory. Po nahradení pôvodnej linky (odkazu) kedykoľvek sa používateľ pokúša na správnu stránku je tajne presmerovaný na zrkadlovú stránku bez toho aby zadal do príkazového riadku prehliadača nesprávnu adresu.

Baiting je niečo ako trojský kôň používajúci prenositeľné fyzické média(cd, usb a pod.) a zneužívajúci chamtivosť obete. Pri tomto útoku zanechá útočník médium pohodené na mieste kde ho určite obeť nájde, poprípade ho označí menovkou alebo firemným logom. Po pripojení tohto média do firemnej siete cez počítač obete, sa vykoná škodlivý malware, ktorý buď pozberá dôležité informácie ako dokumenty, heslá a maily alebo niektoré dokumenty vymaže. Obeť si pritom ale nemusí ničoho všimnúť.

Whaling je nový a silnejšia metóda ako posledné dve. Používa sa na vymáhanie prihlasovacích alebo iných informácií od „väčších rýb“. Často to bývajú ľudia na výkonných postoch a manažéri. Útok neprebieha masovo, ale zameriava sa na túto jednu veľkú obeť. Obeť býva kontaktovaná často personalizovanými emaily upravenými presne na informácie obete. Po nadviazaní prvé kontaktu môže útočník poslať v prílohe podvodnú prílohu, ktorou si zabezpečí vzdialený prístup k počítaču obete. Techník whalingu je viacero a využívajú sa pri nich viacero podvodných postupov zároveň (taktiež prvkov sociálneho inžinierstva).

3.4. Sociálne inžinierstvo

Sociálne inžinierstvo je vlastne metóda, pri ktorej útočník zmanipuluje osobu za účelom vykonania určitej činnosti, pripadne získania údajov. Pri vykonávaní tejto metódy sa používajú mnohé sociotechniky, ktorými útočník dokáže vo svoj prospech namotať. Táto metóda je používaná pri viacerých druhoch malwaru, ktoré sme si prebrali vyššie.

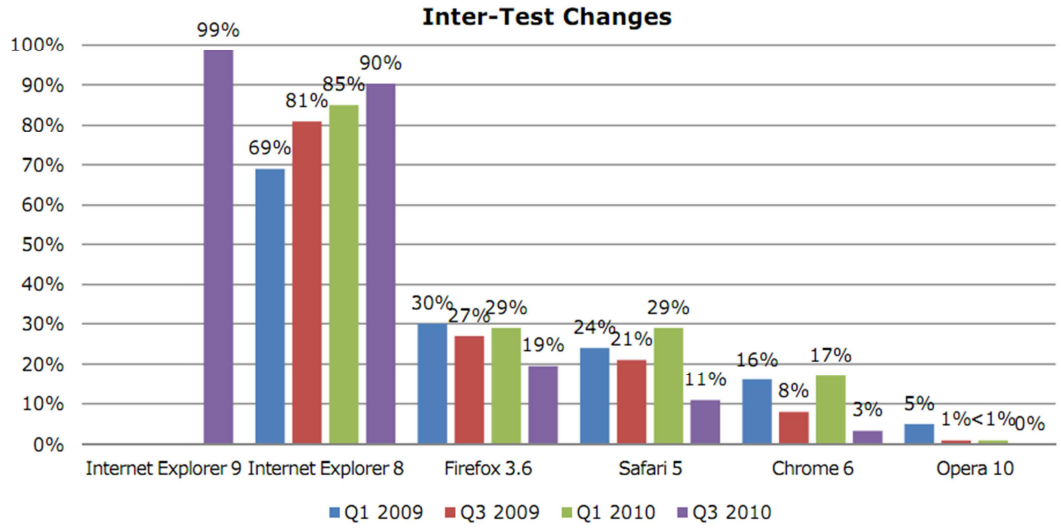
Ľudská slabosť, lakomstvo alebo štedrosť je cesta ktorou sa dajú od ľudí vymámiť všetky potrebné informácie na to, aby mohol byť nejaký podvod zrealizovaný. Je samozrejmé, že takáto pasca musí byť nevyhnutne dobre premyslená a podložená „pravdivými a hodnovernými“ informáciami, ktoré dostatočne zahmlia skutočnosť.

Ako príklad takýchto trikov môžeme uviesť:

- prevod prostriedkov z „prefakturovanej “ objednávky
- pomoc pri úteku z krajiny
- pomoc pri získaní časti zo „zabudnutých“ peňazí bývalého diktátora
- pranie špinavých peňazí

- dary na charitu
- možnosť výhry po zavolaní na konkrétne telefónne číslo a pod.

Podľa rebríčka NSS Labs pomáhajú pred útokmi sociálneho inžinierstva najúčinnejšie chrániť prehliadače Internet Explorer, pričom zatiaľ posledná finálna verzia Internet Explorera 8 dokázala zablokovať 90% útokov sociálneho inžinierstva a súčasná beta verzia Internet Explorera 9 dokonca 99% týchto útokov [2] (viď Obrázok 2).



Obrázok 2 - test ochrany pred útokmy sociálneho inžinierstva v v súčasných prehliadačoch [2]

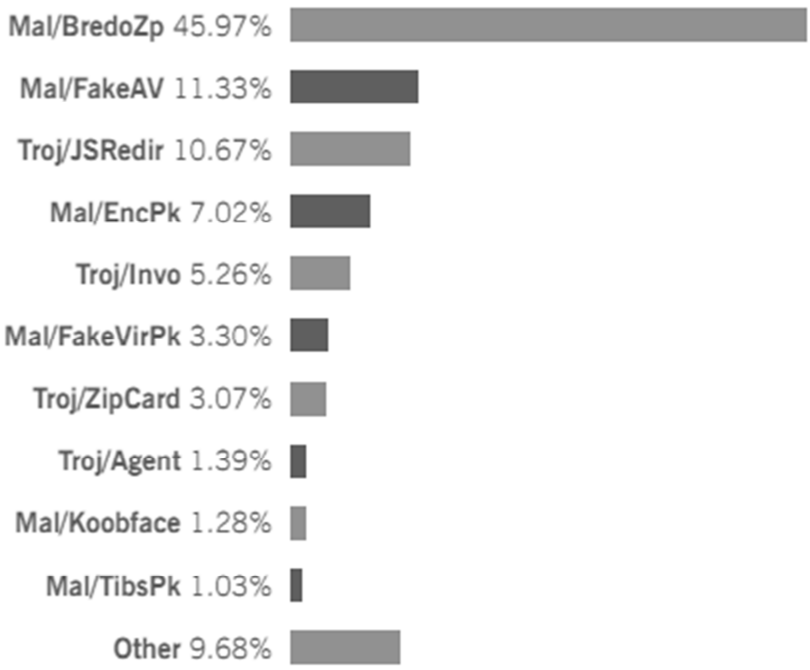
3.5. Mailové nebezpečenstvo

E-mailové správy sú a vždy boli obľúbeným médiom na šírenie malwaru. Stále sa šíria maily s kontroverznými predmetmi správ a pre užívateľa vraj veľmi zaujímavými odkazmi v texte správy. Tieto odkazy smerujú na záškodnícke stránky s malwarom (ako napr. spomínaný Koobface), kde si používateľ stiahne a nainštaluje záškodnícku aplikáciu.

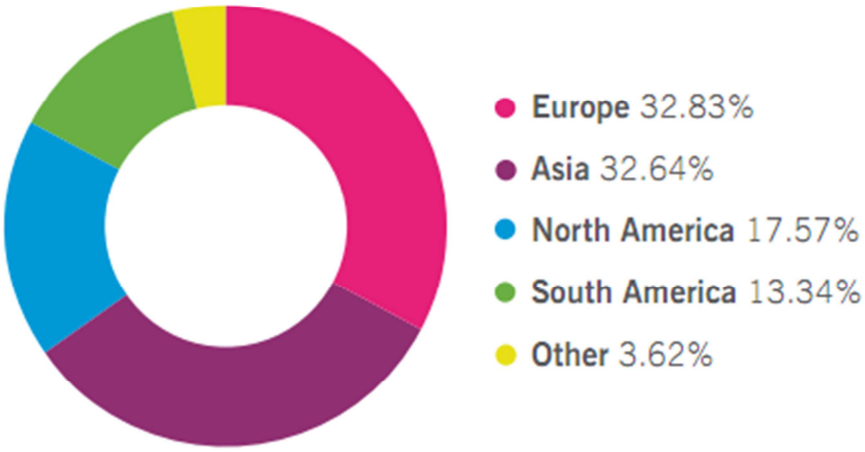
Drvivú väčšinu emailových správ tvorí teda spam, alebo nevyžiadaná pošta s ponukami rôznych výrobkov, výhier a služieb. Podobné problémy začínajú postihovať čoraz viac aj mobilné zariadenia vo forme tzv. Sphamu. V súčasnosti sa miera spamu pohybuje na úrovni 84 až 87 percent zo všetkých mailov [3].

Ako vidieť v grafe najrozšírenejších malwarových hrozieb šírených v prílohách mailov na obrázku Obrázok 3, vo veľkom predstihu dominuje malware Bredolab. Bredo sa v prílohách maskuje za faktúry neexistujúcich objednávok od spoločností DHL, FedEx alebo UPS. Napadnuté počítače sú zapojené do spoločnej botnetovej siete. Tento botnet sa podarilo v priebehu novembra 2010 rozobrať a už nie je schopný byť spravovaný centrálne. V tejto dobe bolo v botnete infikovaných 30 miliónov zombie počítačov.

Druhý malware v poradí, FakeAV láka svoje obete maily s prílohami s 30 dňovou skúšobnou verziou antivírusového program McAfee.



Obrázok 3 - top 10 malware šírený cez e-maily pre jún 2010 [1]



Obrázok 4 - množstvo spamu podla kontinentu

4. Záver

Mnohí ľudia si ešte stále neuvedomujú aké nebezpečenstvo predstavujú škodlivé kódy a malware. Nedostatočne alebo dokonca vôbec nevyužívajú antivírusové programy, firewally a ďalšie ochranné programy, ktoré im počítač ochránia pred nežiadanou infiltráciou. Často potom niektorí z nich prídu o svoje prihlasovacie údaje nielen k herným serverom alebo emailom. Môže sa stať, že autor infiltrácie získa prístup k internet bankingu používateľa a ten tak príde o svoje peniaze.

V súčasnej dobe samotné antivírusové systémy nie sú postačujúce pre detekciu škodlivého kódu. Preto je potrebné zaopatriť ďalšie nástroje zabezpečujúce antiphisingovú, antispamovú, antispywareovú resp. firewallovú ochranu. Používateľ sa môže rozhodnúť pre samostatné aplikácie realizujúce niektoré zo spomínaných ochrán, alebo si vyberie balík poskytujúci komplexné služby v ochrane proti škodlivému kódu.

Je veľmi dôležité oboznamovať ľudí s následkami vírusových infiltrácií a presvedčiť ich, aby si svoje súkromie na počítačoch dostatočne chránili a nebrali to na ľahkú váhu.

5. Predpokladaná literatúra

1. **Sophos.** *Security Threat Report: Mid-year 2010 .* s.l. : Sophos Group, 2010.

2. **Labs, NSS.** *WEB BROWSER SECURITY - Socially-engineered malware protection.* [Online] http://www.nsslabs.com/assets/noreg-reports/NSS%20Labs_Q32010_Browser-SEM.pdf.

3. **Phifer, Lisa.** Top 10 Email Malware Threats. [Online] eSecurity Planet, 2010. http://www.esecurityplanet.com/views/article.php/3903881/Top-10-Email-Malware-Threats.htm.

4. **Shields, Greg.** *Modern Malware Threats and Countermeasures.* s.l. : Sunbelt Software, 2008.

5. **Baratz, Adam.** *Malware: what it is and how to prevent it.* 2004.

6. **Claburn, Thomas.** Top 11 Malware Threats To Watch Out For. [Online] InformationWeek, 2009. http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=206105996.

7. **McAfee.** Latest Malware threats. [Online] McAfee TrustedSource. http://www.trustedsource.org/en/threats/malware_threat.

8. **Gillis, Tom.** *Securing the Borderless Network: Security for the Web 2.0 World.* s.l. : Cisco Press, 2010.