tento text vznikol vznikol v 2008, hrozby odvtedy pribudli

1. BEZPEČNOSŤ NA INTERNETE 3
1.1. MALWARE 4
1.1.1. Vírusy 4
1.1.2. Červy 7
1.1.3. Vsuvka o bezpečnostnej chybe pretečenie zásobníka 8
1.1.4. Trójsky kôň 8
1.1.5. Botnet 9
1.1.6. Rootkit 10
1.1.7. Backdoor – zadné dvierka 11
1.1.8. Adware 11
1.1.9. Spyware 11
1.1.10. Dialer 12
1.1.11. Browser hijacking 12
1.2. NESOFTVÉROVÉ INTERNETOVÉ HROZBY 13
1.2.1. Sociálne inžinierstvo 13
1.2.2. Phishing 14
1.2.3. Pharming 16
1.2.4. Scam 19
1.2.5. Spam 20
1.2.6. Pump and Dump 23
1.2.7. Hoax – poplašná správa 23
1.3. PREČO EXISTUJE MALWARE 24
1.4. OCHRANA PRED MALWARE 26
1.4.1. Antivírusový program 27
1.4.2. Firewall 28
1.4.3. Antispyware, antiadware 29
1.4.4. Aktualizácie 29
1.4.5. Ochrana všeobecne 30
1.5. ZÁVER - BUDÚCNOSŤ MALWARE 30

1. Bezpečnosť na Internete

Čo by z toho chrípka mala,
keby ma nakazila

Peter Adamko

Čo by z toho chrípka mala, keby ma nakazila? Tak táto myšlienka ma napadne vždy, keď počujem, ako niekto (a nie je takých málo) obhajuje svoje slabé zabezpečenie počítača vetou: „Čo by z toho vírus (hacker, resp. čokoľvek iného) mal, keby ma napadol. Nemám v počítači nič cenného.“ Alebo: „Prečo by napadol práve mňa, Jožka Mrkvičku? Ako ma môže poznať?“

Skutočnosť sa má tak, že tak, ako chrípkový vírus nepozná Jožka Mrkvičku, tak ho nepozná hacker alebo zlomyseľný program. A rovnako ho bez zoznámenia nájde – na mene nezáleží. A čo z toho počítačový vírus môže mať? To isté čo vírus chrípky, splní svoje poslania, ktoré sú v zásade rovnaké: rozmnožovať sa a škodiť (aj keď pri chrípkovom víruse je škodenie zrejme len vedľajší efekt prežitia samotného vírusu).

Škodenie už dávno neznamená reštartovanie počítača, mazanie či šifrovanie súborov alebo formátovanie disku. Bohužiaľ. Kedysi bolo dobre. Dnes ide o peniaze.

Podľa firmy Symantec sú čoraz badateľnejšie príznaky, že škodlivé aktivity sa stávajú profesionálnejšie a komerčnejšie. Dokladá to nárastom ekonomických serverov podsvetia, ponúkajúcich ukradnuté informácie. Tieto informácie sa najčastejšie používajú s cieľom odcudzenia identity. V prvom polroku 2007 išlo najčastejšie o čísla kreditných kariet (cena 0,5 – 5 dolárov), bankové účty (30-400 dolárov) či emailové adresy (2-4 doláre za MB).

To, že nejde len o nafúknutú bublinu ale rapídne narastanie nebezpečenstva na Internete dokumentuje aj spoločnosť F-Secure. Spoločnosť oznámila, že v roku 2007 zachytila rovnaké množstvo škodlivého softvéru, ako za posledných dvadsať rokov dohromady[1], t. j. približne 250 000 vzoriek. Skutočnosť potvrdzuje aj firma Symantec, ktorá len v prvom polroku 2007 detekovala viac ako 212 000 nových škodlivých softvérov.

Nárast je zapríčinený aj tým, že tvorcovia vytvárajú rôzne variácie alebo nechajú samotný softvér, nech vyrába mutácie. Dôvodom je snaha sťažiť detekciu svojich produktov.

[1] http://www.networkworld.com/news/2007/120407-f-secure-malware-samples-doubled-in.html

Pritom v roku 1986 bol známy iba jeden počítačový vírus, o tri roky neskôr sa ich počet zvýšil na šesť. V roku 1990 ich už bolo 80 a v roku 1999 sa každý deň objavilo 10 až 15 nových vírusov[2].

O tom, čo sa môže prihodiť neopatrným, neskúseným a hlavne nezabezpečeným používateľom Internetu a tomu ako sa proti rôznym hrozbám brániť je venovaná táto kapitola.

1.1. Malware

Softvér, vytvorený na účel škodenia sa nazýva **malicious software**, z čoho vzniklo slovo používané pre všetky zlomyseľné, škodlivé programy **malware**. V tejto kapitole sú stručne popísané jednotlivé druhy malware. Aj keď je nasledujúce členenie striktné, v praxi sa častejšie vyskytujú rôzne varianty, ktoré majú črty viacerých typov malware.

Malware môže mať rôzne prejavy od jednoduchého obťažovania reklamnými pop-up oknami (pop-up advertising) po ovládnutie počítača s následným kradnutím hesiel alebo sťahovaním ďalšieho malware do počítača.

1.1.1. Vírusy

Vírus je historicky prvým zo škodiacich programov. Patrí mu prvenstvo aj v tom, že o ňom čo-to vie najviac ľudí. Vírus je počítačový program, ktorý je schopný pripojiť sa k nejakému inému programu. Keď používateľ spustí takto pozmenený program, spustí sa najskôr samotný vírus. Keď urobí, čo potrebuje (najčastejšie sa pokúsi nakaziť ďalší súbor na disku, prípadne prevedie nejakú škodlivú činnosť), tak potom spustí pôvodný program. Pretože samotné akcie vírusu sú väčšinou krátke, používateľ si nič podozrivé nevšimne. Vírusy sú teda akýsi príživníci, bez hostiteľa neprežijú.

Proti vírusom sa používajú antivírusové programy. Historicky prvé antivírusové programy používali **vzorky známych vírusov**[3], ktoré potom hľadali v súboroch. Všetko fungovalo ale takýto postup platil (a doteraz platí) iba pri známych vírusoch. Neznámy vírus sa takýmto postupom nedal zachytiť[4]. Preto sa zaviedol nový spôsob boja a to tak, že sa ku každému súboru vypočítal jeho **kontrolný súčet**[5]. Pri kontrole sa už nehľadali len vzorky známych vírusov ale zároveň sa kontrolovalo, či súbor nie je zmenený, t. j. či sa nezmenil kontrolný súčet. Tento postup bol ale nevýhodný v tom, že vytváranie kontrolných súčtov zdržovalo.

---

[2] http://www.symantec.com/avcenter/reference/security.for.web.pdf

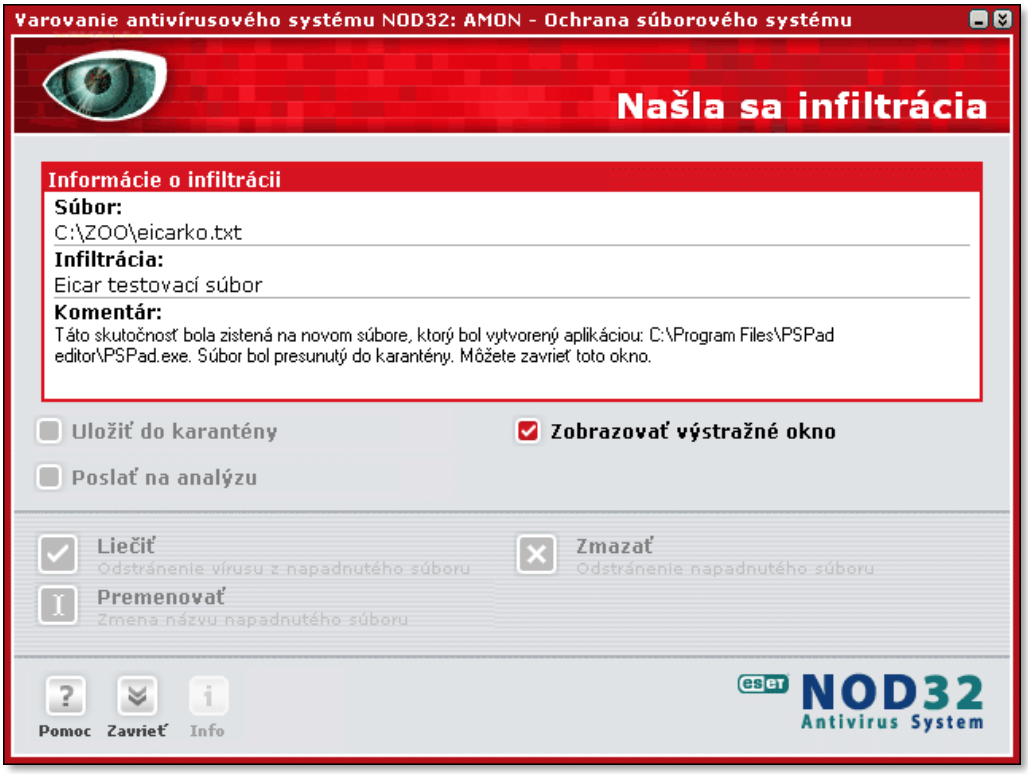
[3] Vírus je program, program je postupnosť čísel. V každom programe sa dá nájsť skupina čísel, ktorá program identifikuje - vzorka. Dá sa povedať, že špecifické činnosti sú kódované špecifickou skupinou inštrukcií.

[4] V dávnych počítačových dobách sa aktualizácie antivírusových programov vydávali raz za mesiac, v súčasnosti aj niekoľkokrát za deň.

[5] Ak považujeme program (ľubovoľný súbor) za postupnosť čísel, možno tieto čísla (nejakým spôsobom) sčítať.

Vírusy sa prispôsobili. Vznikli **rezidentné vírusy**. Po spustení nakazeného súboru (niekedy už po štarte počítača) ostávali v pamäti a klamali antivírusový program. Keď chcel od operačného systému, aby mu oznámil obsah súboru, tak výsledok sfalšovali a antivírusový program dostal pôvodný obsah.

Niektoré vírusy, takzvané **retrovírusy**, šli až tak ďaleko, že ak zistili, že v počítači je antivírusový program, tak ho znefunkčnili. Antivírusový program mohol vyzerať akoby fungoval, ale neoznamoval žiadne vírusy. Aj preto vznikol **EICAR**. Je to krátky program[6], ktorý po spustení vypíše, že je eicar. Nie je to vírus ale každý antivírusový program musí jeho výskyt zaregistrovať a nahlásiť.



Obr. 1.1. Antivírusový program NOD32 odhalil EICAR

Otestujte si svoj antivírusový program. Dajte do Google hľadať slovo eicar a stiahnite prvý súbor, ktorý nájdete. Alebo si ho stiahnite z adresy http://www.eicar.org/anti_virus_test_file.htm. Eicar vyzerá nasledujúco:

[6] Vyskytuje sa aj vo forme nespustiteľného súboru.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Ani so vzorkami známych vírusov to nemali antivírusové programy ľahké. Vznikli **polymorfné vírusy**. Sú to vírusy, ktoré do svojho kódu pridávajú balast[7], neukladajú sa do hostiteľského programu v kuse ale sa rozkúskujú a uložia sa na rôzne pozície. Zakaždým sa uložia na iné miesta a zakaždým pridajú iný balast. Zároveň začali vírusy vznikať čoraz rýchlejšie a kým výrobca vydal aktualizáciu (nové vzorky), stihli nové vírusy nakaziť mnoho počítačov.

Odpoveďou bola **proaktívna ochrana**. Jednou jej formou je **heuristická analýza**. Antivírusový program prezerá súbor a hľadá podozrivé kombinácie príkazov. Druhou formou je **behaviorálna analýza**, ktorá funguje tak, že antivírusový program spustí program vo svojom vlastnom prostredí a skúma či sa nespráva nepatrične. Tieto postupy sú zložitá vec a preto sa môže stať, že antivírusový program označí napadnutý súbor za neškodný (false negative) alebo neškodný súbor za podozrivý (false positive). Kvalita antivírusového programu sa okrem schopnosti spoznať a odstrániť vírus určuje aj podľa počtu falošných poplachov.

Zvláštnou kapitolou boli a sú **makrovírusy**. Do čias keď Microsoft nezabudoval do svojho produktu makrojazyk sa vírusy prenášali iba pomocou programov. V textových súboroch sa nemali ako spustiť. S podporou makrojazyka VBA sa im otvorila cesta aj do dokumentov MS Office.

Ďalšou nepríjemnou technikou súčasnosti je takzvaný **x-morfizmus**. V pôvodných polymorfných vírusoch bol modifikačný podprogram v tele vírusu, čo uľahčovalo antivírusovým programom detekciu (vírusy aj keď boli z veľkej časti rôzne mali spoločnú túto časť). V snahe vyhnúť sa detekcii na základe modifikačnej časti sa súčasný malware (nielen vírusy) začína obmieňať na serveroch, ktoré obsahujú modifikačnú časť a do sveta sa distribuuje iba samotný modifikovaný malware v tisícoch variantoch.

Aby sa detekcia ešte viac skomplikovala, nový malware je často naprogramovaný vo vyšších programovacích jazykoch (pôvodné vírusy boli programované v asembleri). Vyššie programovacie jazyky produkujú viac kódu, ktorý pôsobí ako prirodzený balast.

Najčastejšou akciou vírusov bolo škodenie: mazanie súborov, formátovanie disku. Väčšina škodlivých akcií sa vykonávala v nejaké konkrétne dni, v ostatné dni sa len rozširovali. Našli sa aj pseudo-vtipné: tajne prehodili niekoľko písmen v textových súboroch, niekoľko číslic v číslach, podchvíľou vypínali niektoré klávesy atď.

Dnes sú vírusy (hlavne tie deštrukčné) na ústupe. Čoraz viac sa spájajú s inými formami malware. Skúsenosti nadobudnuté pri ich vývoji sa však bohužiaľ nestratili - využívajú ich tvorcovia ostatného malware.

---

[7] Inštrukcie alebo postupnosť inštrukcií, ktoré nič podstatného nemenia. Napríklad názorný balast z programu na riadenie kráčajúceho robota: „krok dopredu, krok dozadu“ alebo „krok dopredu, krok doprava, krok dozadu, krok doľava“. Nič zložitého ale možností sú tisíce a to znemožňuje vytvorenie vzorky pre konkrétny vírus.

Dôvodom ústupu vírusov je hlavne fakt, že ich základný princíp – rozmnožovanie je pomerne ľahko identifikovateľný. V súčasnosti sa na rozširovanie malware používajú iné prostriedky, najčastejšie ľudská naivita, počítačová nevzdelanosť, neopatrnosť alebo ziskuchtivosť[8]. Z iného súdka je na rozširovanie malware využívať bezpečnostné chyby v programoch. Aj o tom sú dve nasledujúce kapitoly.

1.1.2. Červy

Červ je program, ktorý sa šíri po sieti a napáda zraniteľné a nechránené systémy. Najčastejšie je to operačný systém alebo nejaká sieťová aplikácia (internetový prehliadač, komunikačný program, klient výmennej siete a pod.), ktoré obsahujú zneužiteľnú chybu alebo využíva zdieľané a nechránené disky.

Na rozdiel od vírusu, červ nepotrebuje hostiteľa. Ďalším rozdielom je, že vírus sa šíri iba v rámci jedného počítača a na prenos na iný potrebuje asistenciu človeka alebo iného malware. Červ si dokáže obete na sieti (lokálnej alebo Internete) nájsť sám, prípadne sa sám odošle na emailové adresy, ktoré nájde v kontaktoch poštového klienta nakazeného počítača.

Naprogramovať vírus nie je ani pre priemerného programátora nič ťažké[9], ale naprogramovať červa je už ťažšie. Ťažkosť súvisí s tým, že červ potrebuje na svoje rozširovanie počítače, ktoré majú bezpečnostnú dieru. Autor programujúci červa musí vedieť, že existuje takáto diera a musí ju byť schopný využiť.

Červ si hľadá po sieti vhodné obete a keď nejakú nájde, tak ju napadne a hľadá ďalšie obete aj z nej. Môže pritom upraviť systém tak, aby sa dostal k slovu aj po reštarte. Existujú ale aj také, ktoré sú len v pamäti a na disk sa neukladajú z dôvodu minimalizácie prezradenia. Takéto červy sa využívajú hlavne proti serverom, o ktorých sa nepredpokladá časté reštartovanie.

Hlavnou hrozbou červov (nech už robia čokoľvek) je ich rýchlosť. Na šírenie, na rozdiel od vírusov, nepotrebujú, aby ich niekto spustil. Po prvotnom spustení sa šíria samy bez ľudského zásahu. Rýchlosť ich šírenia závisí len od množstva zraniteľných systémov. Červ sa v ideálnom (a nepríjemnom) prípade rozšíri po celej planéte za pár minút.

Červ môže obsahovať aj ďalšie škodlivé programy, napr. často inštaluje takzvané zadné vrátka – backdoor, ktoré sú popísané v kapitole 1.1.7. Ale aj červ bez doplnkov môže spôsobiť veľké škody. V dôsledku svojej obrovskej rýchlosti šírenia môže červ kompletne zahltiť ľubovoľnú sieť, od LAN až po Internet.

Proti červom pomáha hlavne používať pravidelne a často aktualizovaný operačný systém ako aj ostatný softvér. Pretože niektoré chyby môžu byť známe (niektorým ľuďom) po-

[8] Kto nikdy nepoužil neoprávnene nejaký softvér, nech prvý hodí kameňom.

[9] Ťažšie je naprogramovať ho tak, aby ho nezachytil antivírusový program ☺

merne dlho pred ich opravou, je nutnosťou používanie firewallu. Funkcie firewallu sú popísané v kapitole 1.4.2.

1.1.3. Vsuvka o bezpečnostnej chybe pretečenie zásobníka

Každý program potrebuje nejaké vstupné dáta. Buď ich zadá priamo používateľ alebo si ich program načíta zo súboru v počítači alebo z Internetu. Tieto dáta si počítač musí pred spracovaním uložiť niekde do pamäte. Preto si v pamäti vytvorí pre ne miesto. Ak bude napríklad overovať rodné číslo (rr mm dd vxyz), vyhradí si preň desať znakov. Problém, na ktorý sa dlho neprišlo (ľudia boli asi kedysi čestnejší), nastane, keď je programu podsunutých znakov viac ako očakáva. Ak si program neoveril počet znakov a uložil dáta na vyhradené miesto, tak prepísal časť sám seba. Nad miestom vyčlenenom pre dáta je adresa programu, kde sa má pokračovať. Táto adresa je ale pri vložení „nadrozmerných“ dát premazaná. Niekto si všimol, že keď podstrčené dáta vhodne upraví, tak sa na miesto, kde bola pôvodná adresa môže dostať ľubovoľná iná adresa. A keď v dátach pošle program (všetko je číslo), tak tá adresa môže ukazovať na začiatok tohto programu. A program môže robiť čokoľvek. Teda v závislosti od toho, s akými právami bol spustený zneužitý program.

Preto sa tak často kladie dôraz na to, aby sa používatelia neprihlasovali pri bežnej práci ako administrátori. Nie je to síce 100% riešenie, lebo niektoré programy (napríklad firewall) musia bežať s vysokými oprávneniami, ale v každom prípade sa použitím účtu s obmedzenými právami znižuje riziko nakazenia počítača.

Dáta posielané programu s cieľom využiť túto chybu sa nazývajú exploit. Na Internete si je možné on-line automaticky zostaviť exploit pre ľubovoľný operačný systém a procesor. Stačí nájsť len zneužiteľný program.

Vo Windows XP a vyšších je možnosť **Zabránenie spusteniu údajov (DEP)**, čo je ochrana proti zneužitiu tejto chyby. Niektoré počítačové procesory poskytujú aj hardvérovú podobu tejto funkcie.

Rôzne obmeny tejto chyby boli doteraz asi druhým najčastejším dôvodom nakazenia počítača. Prvým je sám používateľ.

1.1.4. Trójsky kôň

Trójsky kôň je typ malware, ktorý sa maskuje tak, že sa vydáva za niečo zaujímavé alebo užitočné. Na rozdiel od vírusov alebo červov nemá trójsky kôň zvyčajne schopnosť rozmnožovať sa. Po spustení okrem svojej nekalej činnosti môže aj splniť to čo používateľ predpokladá, že by mal robiť. Niektoré trójske kone sa po spustení vyhovoria na chýbajúcu knižnicu alebo poškodený súbor. Najčastejšou funkciou je inštalovanie tzv. backdooru (zadných vrátok) alebo zachytávanie a posielanie stlačených kláves (keylogger).

Trójsky kôň sa dostane do počítača rovnako ako sa vzor, po ktorom bol pomenovaný, dostal za hradby Tróje. Teda **pričinením samotného používateľa**, ktorý ho dotiahne (stiahne) do počítača, pričom je schopný vypnúť všetky ochrany, ktoré má – len aby ho spustil. Ukáž-

kovým príkladom je snaha spustiť crack, aby mohol používať zadarmo chránený program alebo hru.

Podľa firmy Symantec počas prvého polroka 2007, trójske kone zaberali v rebríčku TOP 50 malware až 54%.

1.1.5. Botnet

Svet literárneho a filmového hororu poskytol svetu počítačov meno **zombie**. Zombie sú bezduché mŕtve bytosti, najčastejšie mŕtvi ľudia, ktorí sa ale správajú (s troškou fantázie) ako keby boli živí. Možno sú živí ale sú pomalí, apatickí, nemajú o nič záujem. Iba ak o to ako škodiť – zabíjať, či skôr meniť živých a normálnych na zombie. V hororoch sa vyskytujú vo veľkých množstvách, čo z nich robí nepríjemnú hrozbu, ktorú nemožno ignorovať.

V počítačovom svete je to rovnaké. Alebo horšie. Zombie vo filme rozoznáte na prvý pohľad. Počítač - zombie nemusíte, pokiaľ nie ste odborník, odhaliť vôbec. Názov botnet sa dá preložiť ako sieť robotov (skratka bot sa často požíva namiesto robot), počúvajúcich príkazy. Iný výklad – sieť riadená robotom, vychádza zo skutočnosti, že prvé botnety boli riadené cez IRC, kde sa o zombie staral špeciálne vytvorený program - robot. Hackeri spravujúci botnety sa nazývajú bot herders – pasáci.

Bohužiaľ spôsob, akým sa vo filmoch a v knihách hrdinovia zbavia zombie, sa v počítačovom svete nedá použiť. A zombie sú tu. **Vo veľkých množstvách**. Nie sú výnimkou siete zombie, ktoré obsahujú státisíce počítačov[10].

Ako to funguje? Nejaký malware, najčastejšie červ alebo trójsky kôň, nainštaluje program, ktorý vykonáva príkazy, ktoré sú mu na diaľku zadávané. Teda počítač už nie je plne pod kontrolou používateľa. Funguje akoby sa nič nestalo, ale kedykoľvek môže urobiť čokoľvek.

Prvé botnety boli pôvodne ovládané centrálne z jedného servera, kam si „chodili“ alebo odkiaľ dostávali v nejakých intervaloch inštrukcie. To malo ale zásadnú slabinu v tom, že ak sa server vyradil z činnosti, neurobili už nič. Preto počítače v novších botnetoch komunikujú spôsobom peer-to-peer. Hackerovi sa stačí napojiť na jeden zombie-počítač, z ktorého sa potom inštrukcie šíria lavínovite k ostatným.

Nakazený počítač si na základe inštrukcií dokáže stiahnuť ďalší malware, ktorý potrebuje pre svoju činnosť. Je schopný aktualizovať sa, a tak predísť odhaleniu.

Zombie dnes rozosielajú viac ako 60% spamu. V prípade, že by spam rozosielali normálne poštové servery, bolo by možné ich zablokovať ale ako zablokovať státisíce počítačov?

[10] http://blog.trendmicro.com/category/botnet/

Spoločnosť Symantec zistila v prvej polovici roku 2007 v priemere 52 771 aktívnych zombie počítačov denne. Priemerná dĺžka života zombie sa predĺžila v porovnaní s predchádzajúcim polrokom z troch na štyri dni – čo ale nemusí byť presný údaj – zombie počítač mohol byť len neaktívny.

Asi najväčšiu botnet roku 2007 založil červ Storm. Storm sa začal rozširovať v januári 2007. Meno mu bolo pridelené na základe jeho spôsobu šírenia. Maskoval sa tým, že v e-maile sľuboval informácie o cyklóne (anglicky storm)[11]. Tí, ktorí uverili, si stiahli trójskeho koňa, ktorý zmenil ich počítač v zombie. Odhaduje sa, že v októbri 2007 mala botnet Storm jeden milión zombie členov.

Sieť sa postupne rozpadla (zámerne) na menšie celky. Predpokladá sa, že dôvodom je ľahšie spravovanie a aj snaha autorov predať jednotlivé podsiete (hlavní kupci sú spameri a DDoS[12] útočníci). Ostatný variant používa šifrovanú komunikáciu cez sieť typu peer-to-peer, pomocou ktorej počítače jednotlivých podsietí navzájom komunikujú.

1.1.6. Rootkit

Rootkit je špeciálny typ malware, ktorý dokáže ukryť seba ale prípadne aj iné programy v napadnutom systéme, a tak zabrániť detekcii. Rootkit sám o sebe nemá význam, preto býva kombinovaný s iným škodlivým softvérom, najčastejšie s backdoor alebo spyware. Pri rootkitoch najdôležitejšia prevencia, čiže schopnosť proaktívne zastaviť pokus o vniknutie do systému. Rootkit sa dokáže v systéme po svojej aktivácii „zneviditeľniť“ a užívateľ napadnutého počítača tak môže získať falošný pocit bezpečia.

Rootkit nevyužívali len hackeri. V roku 2005 Sony BMG Music Entertainment použila rootkit na zamaskovanie svojho softvéru pre DRM (Digital Rights Management), ktorý sa nahral do počítača po vložení CD a mal chrániť autorské práva. Problémom bolo (okrem tajnej inštalácie), že rootkit umožňoval pomerne jednoduché ukrytie ľubovoľného softvéru, čo samo-

---

[11] To je bežná prax, keď sa objaví živelná pohroma, ľudia chcú byť informovaní. A e-maily s nákladom malware to využívajú. V prípade, že sa dlhšie nič nedeje, tak sa nejaká udalosť vymyslí. Ďalšie vlny posielali napríklad „informácie“ o nukleárnom teroristickom útoku. Dobre funguje oznam o zadržaní Usáma bin Ladina alebo samovraždе nejakej svetoznámej celebrity.

[12] DoS – Denial of Service (odopretie služby), DDoS - Distributed DoS (mnohonásobný DoS). Mnoho organizácií má podnikanie založené na on-line službách a pre mnohé je to dôležitý doplnok podnikania. Napríklad internetový obchod alebo internetbanking. Server alebo servery firmy sú dimenzované tak, aby zvládli bežný, prípadne s istou rezervou nadštandardný nápor požiadaviek. Ale čo ak bude požiadaviek niekoľkonásobne viac. Servery nebudú stačiť a záujemcovia o nákup, či predaj na internetovom obchode alebo klienti banky, ktorí sa chceli dostať na svoj účet budú odmietnutí. Ak sa to stane viackrát, stratia dôveru v server, prípadne celkom o takýto druh služieb.

Pomocou botnet je jednoduché prikázať desiatkam tisíckam zombie, aby sa snažili prihlásiť (je jedno, že nevedia heslá, hlavne nech server zamestnajú) na www.DakaBanka.xy. To je DDoS. A nech to robia nejakú dobu v kuse. Klienti sú nervózni, ale banka za to nemôže. Za útokom môže byť konkurencia, vydieranie alebo pokus nastrčiť za nedostupný server iný, pre útočníkov „vhodnejší“.

zrejme rôzne skupiny využili. Prípad mal na Internete obrovský ohlas a skončil tak, že spoločnosť musela vydať program, ktorý rootkit odstránil[13].

Na Internete sú ponúkané na predaj rootkity pre každý operačný systém, napríklad aj s možnosťou priplatiť si, za garanciu ich nedetekovateľnosti, prípadne za ich aktualizáciu. Existujú aj open source rootkity, napríklad rootkit FU[14].

1.1.7. Backdoor – zadné dvierka

Backdoor je program umožňujúci vzdialený prístup na počítač. Tento druh programov sa administrátormi normálne používa na vzdialenú správu počítača. Problém nastáva, keď je nainštalovaný a využívaný bez vedomia majiteľa počítača.

Backdoor zvyčajne inštalujú trójske kone alebo červy.

1.1.8. Adware

Adware je softvér, ktorý pri surfovaní po Internete automaticky zobrazuje reklamu. Reklama sa mení v závislosti od stránok, na ktorých sa používateľ nachádza. Adware je často súčasťou programov dostupných zadarmo na Internete ale podmienkou ich bezplatného používania je práve prítomnosť reklamy. Asi najznámejším príkladom je použitie novších verzií prehrávača BSplayer.

Problém nastáva v prípade, keď používateľ pri inštalovaní odkliká všetko čo sa dá a zvyčajne takto nevedomky súhlasí aj s nainštalovaním adware.

1.1.9. Spyware

Spyware je program, ktorý zbiera informácie bez vedomia používateľa. Napríklad o navštívených stránkach, o nainštalovaných programoch, heslách[15] či iných aktivitách a potom ich posiela cez Internet. Podľa rôznych štatistík je spyware napadnutých až 70%-90% počítačov. Toto množstvo je docielené tým, že na seba nijako neupozorňujú, nerozmnožujú sa a priamo neškodia.

---

[13] http://www.cio.com/article/21347

[14] http://www.rootkit.com/project.php?id=12

[15] Je možné zistiť heslá, ktoré sú uložené v počítači. Napríklad heslá uložené poštovým klientom alebo internetovým prehliadačom, pre pohodlnejší prístup na poštový alebo iný server. Spyware môže sledovaním klávesnice zistiť aj heslá, ktoré nie sú nikde uložené a používateľ ich zadáva pri vstupe na nejaký server. Špecializovaný program, ktorý sa venuje takémuto zachytávaniu znakov z klávesnice sa nazýva keylogger. Existuje aj hardvérová podoba keyloggeru. Vyzerá približne ako USB kľúč s konektorom na dvoch stranách. Do jedného konca sa napojí kábel klávesnice a takto predĺžený kábel sa normálne pripojí k počítaču. Všetko, čo prechádza káblom sa zaznamenáva a po čase stačí prísť vybrať alebo vymeniť keylogger a doma si pozrieť, čo všetko používateľ napísal. S keyloggermi súvisia aj programy nazývané screen recorder (tiež nazývané screenlogger), ktoré zaznamenávajú obrázky obrazovky.

Najčastejšia cesta spyware do počítača začína na serveroch s crackmi, sériovými číslami, porno serveroch alebo serveroch umožňujúcich nelegálne sťahovanie hier či hudby. Stávajú sa aj prípady hacknutia serióznych serverov a ich následnej úpravy napríklad tak, aby využívali chyby prehliadačov, a tak umožnili prístup spyware (vo všeobecnosti ľubovoľnému malware) do počítača.

Získané informácie sa dajú využiť pri podvodoch cestou odcudzenia identity – niekto uskutoční obchod/podvod vo vašom mene. Dajú sa využiť aj priamo proti Vám, pomocou niektorej z techník nesoftvérových útokov popísaných v kapitole 1.2.

1.1.10. Dialer

Dialer je program, ktorý presmeruje telefonické pripojenie, prostredníctvom ktorého sa užívateľ pripája na Internet, na iné (drahšie) číslo. Tieto programy sa využívajú aj legálne pri platení za niektoré internetové služby. Problém nastáva, keď sa tak stane bez vedomia používateľa. Používateľ napadnutého počítača potom napríklad surfuje po Internete namiesto cca 20 korún za hodinu, za 100 korún za minútu.

Výskyt tohto malware v súčasnosti je na ústupe, pretože využíva klasické vytáčané pripojenie na Internet, vrátane ISDN. V prípade, že sa na Internet pripájate pomocou DSL, toto nebezpečenstvo Vám nehrozí.

1.1.11. Browser hijacking

Program spôsobujúci Browser hijacking – únos prehliadača má asi najviditeľnejšie a najotravnejšie prejavy zo všetkých malware. Dá sa povedať, že je to jediný malware, ktorého prejavy používatelia vidia a vnímajú ako útok (s výnimkou adware ale ten nebýva taký agresívny).

Je to malware modifikujúci správanie sa internetového prehliadača. Medzi najčastejšie prejavy patrí zmena domovskej stránky (a pre bežného používateľa nemožnosť jej obnovenia), zmena vyhľadávača, presmerovávanie odkazov a tiež ďalšie aktivity patriace do kategórie adware a spyware. Niekedy zobrazuje reklamu oznamujúcu používateľovi „prekvapujúcu“ novinku – že má napadnutý počítač. A samozrejme ponúka predaj programu na odstránenie infekcie.

Do počítača sa dostane najčastejšie snahou používateľa (ako ináč) nainštalovať nejaký program, z neznámeho zdroja, ktorý zadarmo sľubuje neskutočne dobré služby. Je ale možné, že k nainštalovaniu došlo vďaka bezpečnostnej chybe prehliadača alebo nízkej úrovne zabezpečenia.

Tieto programy sa vyznačujú aj tým, že napriek ich viditeľným prejavom ich niekedy nedokáže odinštalovať ani bežný IT odborník. Ich spustenie pri štarte počítača je totiž zabezpečené mnohými spôsobmi a prehliadnutie a neodstránenie čo len jedného z nich, privedie situáciu do pôvodného stavu. V pamäti sú často viaceré kópie jedného malware alebo viacero rôznych malware, ktoré sa vzájomne podporujú a keď odstránite jeden z ich, ostatné ho auto-

maticky opäť spustia. Práve táto ustavičná kontrola, či im niekto nezlikvidoval kolegu, je dôvodom, prečo sú takto postihnuté počítače pomalé – na nič iné ako na kontrolu neostáva čas.

1.2. Nesoftvérové internetové hrozby

Niekedy sa snažia útočníci presvedčiť používateľa, aby si stiahol a nainštaloval ich softvér dôvodom, že bez neho sa stránka nezobrazí správne. Tento jav sa najčastejšie vyskytuje pri serveroch s pornografickým obsahom. Video sa neprehrá[16], ak sa nenainštaluje „kodek". Vynútenie stiahnutia a nainštalovania je v prípade odmietnutia podporené množstvom chybových hlásení a opätovným zobrazovaním výzvy pre inštaláciu.

Niektoré web servery používajú pri komunikácii zabezpečený protokol (https), čím sa snažia vyvolať dojem bezpečia a serióznosti. Protokol je bezpečný ale iba z hľadiska toho, že komunikácia medzi prehliadačom a serverom je šifrovaná a tretia strana, ktorá by na Internete zachytávala túto komunikáciu, nemá prakticky šancu ju rozšifrovať. Tento protokol ale nijako nevypovedá o serióznosti alebo neserióznosti servera na druhej strane komunikačného kanála.

S tým súvisí aj odvolávanie sa na certifikačnú autoritu, ktorá jednoznačne potvrdí, že naozaj ide o server XY. Tento spôsob používajú (mali by používať) banky pri komunikácii s klientom. Certifikačná autorita **potvrdzuje**, že server naozaj je tým serverom, za ktorý sa vydáva. **Nepotvrdzuje** ale kladné úmysly servera.

Ľudia vedia, že ak sa chcú dostať na stránku svojej banky alebo web mailu, musia preukázať (prihlasovacím menom a heslom), že sú oprávnení. Drvivú väčšinu ani nenapadne, že by stránka banky alebo iné servery mali tiež preukázať, že sú naozaj weby týchto inštitúcií. Weby to aj často robia ale používatelia to nekontrolujú, a tak si nevšimnú, keď web banky svoju identitu nepotvrdí. V kapitolách o phishingu a pharmingu je uvedené, že táto neznalosť je naozaj zneužiteľná a aj sa zneužíva. Väčšina uvedených techník využíva metódy známe ako sociálne inžinierstvo, ktoré je popísané v nasledujúcej časti.

1.2.1. Sociálne inžinierstvo

Sociálne inžinierstvo je spôsob získavania peňazí alebo dôverných informácií pomocou manipulácie potenciálnej obete. Táto metóda sa dá využiť prakticky všade: osobný, e-mailový, telefonický kontakt, bežnou poštou alebo pomocou web stránky. Zneužíva sa pritom dôverčivosť ľudí vydávaním sa za známe a existujúce osoby, spoločnosti či inštitúcie. Jeden zo základných pilierov sociálneho inžinierstva je poskytovať potenciálnej obeti informácie, ktoré by rada počula:

(Osobný kontakt) Milá pani, sme naozaj neskutočne šťastní, že sme to my, ktorí Vám prinášame túto radostnú správu.

[16] „Do kelu, zasa počuť iba zvuk."

VYHRALI STE

Vyhrali ste 10 000 000, dobre počujete DESAŤ MILIÓNOV SLOVENSKÝCH KORÚN!! Fotka Vašich vnúčikov obsadila prvé miesto v súťaži, ktorú organizovala naša firma „Deti a hračky“. Máte už premyslené, čo s takým majetkom urobíte? Určite pôjde veľká časť vnúčikom, však? Tu, na tejto fotke vyzerajú roztomilo a veľmi inteligentne.

Čooo? Majú len dva roky a už vedia zapnúť DVD prehrávač, ktorého sa Vy bojíte? No jasné, kúpite im počítač. Každému jeden – ten najlepší. To viete – nová generácia. No a na aký účet Vám poslať peniaze?

Príde Vám tam 8,1 milióna, viete štát si zdaní všetko. Áno, je to hrozné, aspoň dôchodcov by mohol ušetriť. Je tu ale **jedna možnosť** *ako sa tomu vyhnúť – našťastie sa dajú niektoré zákony využiť aj v prospech obyčajných ľudí. Pred samotným vkladom je výhodné zaplatiť správny poplatok 9 500 a výhra bude vedená ako dar a ten sa (ako možno viete) nezdaňuje.*

Ušetríte MILIÓN OSEMSTODEVÄŤDESIATTISÍC PÄŤSTO KORÚN.

Ale aby sme stihli vybaviť formality u notára, pred tým ako prídu na účet peniaze, tak je nutné zaplatiť to hneď. Samozrejme, vybavíme to za Vás. No nemáme Vám ale vydať – Aaach, tak ďakujeme, pripijeme si na Vaše zdravie a samozrejme aj na vnúčikov.

Malý test:

1. Koho máte radšej, toho kto Vás chváli alebo toho, kto Vám nadáva?
2. Ste šťastnejší, keď môžete získať peniaze?
3. Komu skôr uveríte, tomu koho máte radi, či niekomu, koho radi nemáte?
4. Komu dáte svoje peniaze? Jasné, že tomu, komu veríte.

Ak to zjednodušíme, dáte peniaze (alebo aspoň informácie) tomu, kto Vás chváli a s Vami súhlasí a prisľúbi Vám zisk.

Metódy sociálneho inžinierstva používajú odpradávna aj rozliční „veštci“ a „liečitelia“, ktorí Vám vyveštia a vyliečia čokoľvek chcete (ak im o tom poviete). V nasledujúcich kapitolách Phishing, Scam, Pump and dump a Hoax je sociálne inžinierstvo ukázané na reálnych príkladoch.

1.2.2. Phishing

Slovo phishing pochádza z anglického slova fishing (rybárčenie). Rybou – úlovkom sú peniaze alebo dôverné informácie, najčastejšie čísla bankových účtov aj heslami, získané pomocou podvodného emailu. Podvodný e-mail slúži ako háčik, na ktorý sa nachytajú neskúsení alebo neopatrní používatelia.

Scenár pri phishingových emailoch je nasledujúci:

Vážený klient,

na Vašom účte sme zaregistrovali žiadosť, o vyplatenie sumy 11 286,50 Sk na účet vedený na Bahamských ostrovoch, ktorú ste potvrdili pred hodinou z Buenos Aires. Keďže sa domnievame, že môže ísť o podvod, tak Vás vo **Vašom vlastnom záujme** *žiadame, aby ste sa kliknutím na nižšie uvedený odkaz, prihlásili do svojej banky a prípadne uvedenú transakciu zrušili.*

V prípade, že transakciu nezrušíte do zajtra rána 6:00 hod, budeme predpokladať, že transakcia je platná a peniaze budú odoslané.

V prípade, že je transakcia platná, považujte tento email za bezpredmetný.

V prvom rade je treba príjemcu emailu vystrašiť, dostať do tiesne – ľudia v strese nekonajú úplne racionálne. V tomto prípade sa boja, že prídu o svoje peniaze. E-mail vyzerá logicky: Banka má podozrenie a preto je opatrná. Aké je to pekné od nej.

Inou formou je zaslanie výherného kódu, ktorý je možný použiť pre nákup na Internete s obrovskou zľavou. Samozrejme, akcia ako na truc, za chvíľu vyprší. Preto sa treba rýchlo prihlásiť a nakupovať. Ziskuchtivosť platí na ľudí rovnako ako strach v predchádzajúcom prípade (koniec koncov, v oboch prípadoch ide o peniaze).

Háčik je už hodený a treba iba čakať, koľko ľudí klikne na odkaz. Odkaz sa často podobá na internetbanking banky, napríklad namiesto paypal.com je paypa1.com (v druhom prípade je namiesto malého písmena L číslica jeden). Inou možnosťou je vytvorenie adresy posunutím domény druhej úrovne do tretej úrovne, napríklad namiesto www.VasaBanka.sk, ponúknuť www.VasaBanka.internetbanking.com. Na falošnej adrese je samozrejme verná kópia webu pravej banky. Alebo sa naozaj otvorí pravá stránka ale pre zadanie hesla sa otvorí iné (pop-up, vyskakovacie) okno z falošnej banky.

To, že sa používa grid karta, nie je pre podvodníkov skoro žiaden problém. Údaje, ktoré zadáva používateľ pri prihlasovaní na webe falošnej banky sa automaticky prepošlú do pravej banky. Pravá banka pošle žiadosť o grid tej falošnej – lebo s ňou komunikuje. Falošná banka posunie žiadosť o verifikáciu používateľovi a jeho odpoveď posunie pravej banke[17].

Tvorca phishingu väčšinou nevie, akú má adresát banku ale to neznamená, že sa nemôže trafiť. Firma Symantec zaregistrovala v prvom polroku 2007 až 196 860 rôznych phishingových správ, za predchádzajúci polrok ich bolo „iba“ 166 248. To znamená v priemere vyše tisíc nových typov správ denne. Z nich 72% bolo zameraných na získanie informácií z finančného sektora.

[17] Popísaná metóda sa volá Man-in-the-middle attack – útok muža v strede, čo celkom vystihuje fungovanie tejto metódy.

V rovnakom období produkty spoločnosti Symantec zablokovali 12,5 milióna phishingových správ denne.

Obete phishingu alebo pharmingu (ktorý je popísaný v nasledujúcej kapitole) možno rozdeliť do dvoch skupín. V prvej skupine sú to používatelia, ktorí takýmto spôsobom prezradili nejaké informácie a prípadne prišli o peniaze (tie im môžu byť v mnohých prípadoch bankou vrátené – z dôvodu neznižovania dôvery v on-line služby). V druhej skupine sú to inštitúcie, ktorých meno bolo zneužité. Aj keď sú v tom často dotyčné organizácie nevinne, dôvera v ich služby rýchlo klesá a straty zo zmarených obchodov a náklady na reklamu na obnovenie dôvery presahujú straty ich klientov.

Podľa prieskumu spoločnosti Gartner, Inc., zaoberajúcou sa prieskumom a analýzou IT priemyslu, prišli americké banky a vydavatelia kariet v roku 2003 o 1,2 miliardy dolárov. Nepriame straty sú omnoho vyššie (odhaduje sa dvojnásobok priamych strát) – hlavne v dôsledku straty dôvery v on-line služby.

Na Slovensku a v Česku nie je phishing zatiaľ príliš rozšírený. Dôvodom je hlavne pomerne malý trh – v porovnaní s lukratívnejšími oblasťami, hlavne USA. Ďalším dôvodom je jazyková bariéra. Ale napriek tomu sa už pár pokusov vyskytlo.

Nejde ale len o to získať pomocou phishingu peniaze priamo, banky sa stávajú tvrdým orieškom. Čoraz častejšie sa cieľom útokov stávajú inštitúcie, kde možno získať dôverné informácie (čísla účtov, Social Security Numbers - u nás rodné čísla, čísla kreditných kariet a pod.), ktoré možno speňažiť alebo použiť pri iných podvodoch.

Dôležitým bodom v obrane pred phishingom je ostražitosť. Okrem toho je dôležité neklikať na odkazy a v takýchto prípadoch (alebo radšej vždy) napísať adresu banky, prípadne inej inštitúcie do internetového prehliadača vlastnoručne. Nepríjemné je keď sa hackerom podarí hacknúť stránku inštitúcie (nemusia sa dostať do systému s heslami alebo kontami) a iba zbierať kontá a heslá ľudí, ktorí sa chcú prihlásiť.

Nová forma, **spear phishing**, využíva informácie o adresátovi (získané napríklad pomocou spyware) a je teda presnejšie zameraná – je cielená. To, že obsahuje dôverné informácie, môže zároveň vzbudiť v obeti dojem, že ich naozaj posiela spoločnosť, ktorá je uvedená ako odosielateľ, a tak je väčšia šanca, že sa dá nachytať.

1.2.3. Pharming

Slabinou phishingu je nutnosť uvádzať falošnú adresu. Snom každého phishera je, aby mohol uvádzať pravú adresu a pritom aby sa používateľ dostal na jeho nepravú stránku. To umožňuje pharming.

Pre pochopenie pharmingu je nutné vedieť ako funguje **DNS** (Domain Name System). Našťastie je vcelku jednoduché. Každý počítač (uzol, zariadenie), ktorý chce komunikovať

v Internete musí mať IP adresu. IP adresa je štvorbytové číslo[18], pričom sú jednotlivé byty oddelené bodkou. Napríklad IP adresa 158.193.180.1 je adresou servera Fakulty PEDaS, Žilinskej univerzity. Pamätať si ale takéto čísla je pre človeka nepohodlné, preto majú niektoré uzly (najčastejšie web servery) priradený slovný (doménový) názov[19]. Napríklad fpedas.uniza.sk je slovný ekvivalent číselnej adresy uvedenej o tri riadky vyššie.

Keď napíšeme do internetového prehliadača fpedas.uniza.sk, tak sa prehliadač pokúsi zistiť, aká IP adresa je priradená k tejto slovnej adrese. Ak IP adresu zistí, tak s uzlom na tejto adrese začne komunikovať a zobrazí nám výsledok – v tomto prípade webové stránky. Ak sa prehliadaču IP adresu nepodarí zistiť, vypíše hlásenie, že stránku nemôže nájsť (stane sa to napríklad aj vtedy, ak pri písaní adresy urobíte preklep) a samozrejme želanú stránku nezobrazí. Z toho je vidieť, že je veľmi dôležité umožniť prehliadaču zistiť zodpovedajúcu IP adresu.

Starajú sa o to DNS servery, ktoré evidujú dvojice: IP adresa - doménová adresa. Ak prehliadač nepozná IP adresu, opýta sa DNS servera. Ten mu, ak vie, odpovie, ak nevie, tak sa (DNS server) opýta ďalšieho DNS servera. A tak to ide ďalej, až kým niektorý DNS server neodpovie.

DNS servery si môžu medzi sebou vymieňať informácie o svojich záznamoch a prípadne si ich jeden podľa druhého upravujú. Toto využívajú hackeri a niekedy sa dokážu dostať do DNS servera, ktorý je slabo zabezpečený alebo obsahuje chybu. Upravia napríklad záznamy bánk tak, že slovné adresy ukazujú na weby falošných bánk.

V takomto prípade a v prípade, že web banky/inštitúcie nemá vyššiu formu zabezpečenia pred neoprávneným prístupom (iba heslom a prípadne grid kartou) nemá človek prakticky žiadnu šancu. Dobrou ochranou je potvrdenie platby inou cestou ako cez Internet, napríklad kontrolnou SMS z banky. Nie je to prehnaná ani výnimočná ochrana, napríklad aj pri autách sa tiež chránime viacnásobne, okrem zamknutia dverí navyše alarmom, zamknutím volantu či imobilizérom.

Tak ako používateľ preukazuje svoju oprávnenosť pre vstup heslom (a prípadne ďalšími mechanizmami) aj banka (alebo iná dôležitá inštitúcia) by mala dokazovať, že je to ona. A mala by to preukázať pred tým, ako používateľ zadá heslo.

Prehliadač si môže, v prípade, že s inštitúciou komunikuje protokolom https, overiť od takzvanej certifikačnej autority, že ide naozaj o web server danej inštitúcie. Ak sa mu webový server nepodarí overiť, tak používateľa varuje. Je ale možné, že napriek tomu je všetko

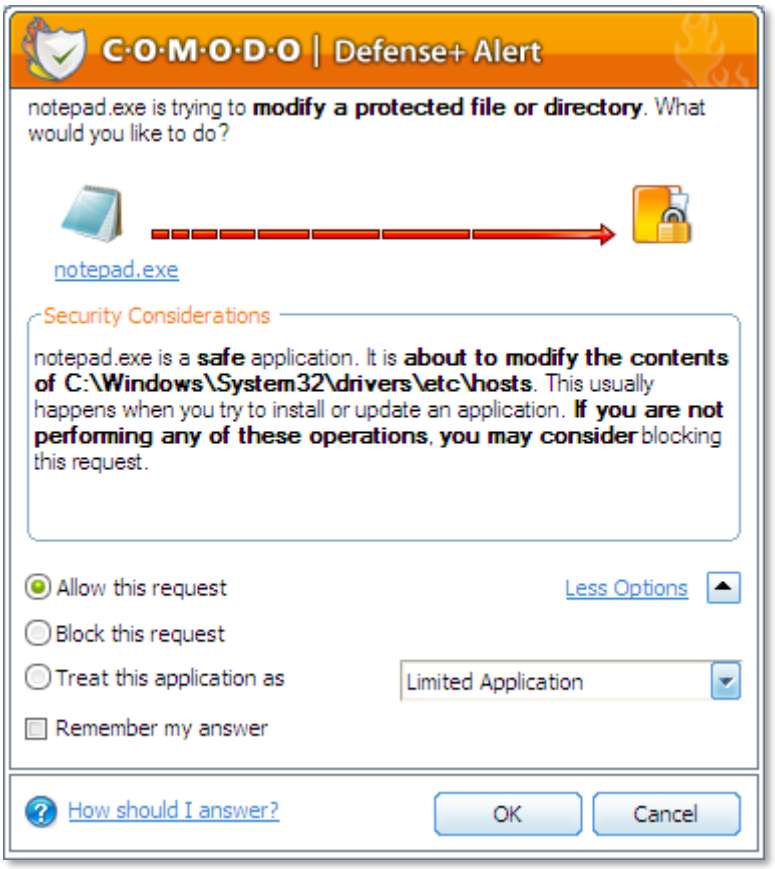
[18] 1 byte je číslo od 0 do 255.

[19] Druhým dôvodom pre doménové názvy je hierarchické členenie. Napríklad uveďme adresu fpedas.uniza.sk. Top level doména sk znamená, že stránka je registrovaná na Slovensku (server môže byť fyzicky aj v inom štáte). Doména druhej úrovne uniza reprezentuje celú univerzitu. A doména tretej úrovne fpedas je určená pre Fakultu PEDaS. Doména tretej úrovne www v prípade www.uniza.sk je iná ako doména štvrtej úrovne www.fpedas.uniza.sk. Doménu www je možné niekedy vynechať, niekedy nie, záleží od konfigurácie servera.

v poriadku. Prehliadač iba nepozná certifikačnú autoritu, ktorá správnosť potvrdzuje. V takom prípade je možné certifikačnú autoritu pridať.

Operačné systémy môžu mať podobné záznamy ako v DNS serveri (samozrejme v menšom meradle). Majú ich hlavne z dôvodu aby sa nemuseli obracať na DNS servery pre často navštevované adresy. Napríklad v MS Windows sa v c:\Windows\System32\drivers\etc\ nachádza súbor hosts. Prehliadač sa ešte pred otázkou na DNS server pozrie do tohto súboru či tu nie je záznam pre hľadanú adresu.

Obsahom súboru hosts je najčastejšie iba dvojica 127.0.0.1 a localhost. Pod týmito adresami sa pozná každý počítač, aj keď má pridelenú inú IP alebo slovnú adresu ale to nás teraz nezaujíma.



Obr. 1.2. Firewall Comodo zistil pokus o zmenu súboru hosts

Názorný príklad ako funguje pharming si môžete **na vlastnú zodpovednosť** a na vlastnej koži vyskúšať aj na svojom počítači. Ale najskôr dočítajte túto kapitolu do konca.

Zapíšte[20] (napríklad v Notepade/Poznámkovom bloku, nie vo Worde!) nakoniec súboru uvedeného v predchádzajúcom odseku, do nového riadku

158.193.180.1 mojabanka.sk

(medzi adresami je medzera alebo tabulátor). Súbor uložte, spusťte internetový prehliadač, napíšte do neho mojabanka.sk. Ak ste všetko zvládli, mali by ste sa ocitnúť na stránke Fakulty PEDaS.

Ak sa Vám podarilo bez problémov zapísať do súboru hosts, tak Váš počítač nie je chránený dostatočne. Takto môže pozmeniť súbor hosts aj nejaký malware, ktorý keď už je v počítači, nemá problém zistiť Vašu banku, zapísať súboru hosts vhodnú dvojicu.

V zápise do súboru hosts by Vám v tom mohol zabrániť (a to by bolo dobre) niektorý z bezpečnostných programov, ktoré používate. V takom prípade sa Vás môže opýtať na povolenie na zápis. Toto povolenie môže byť jednorazové alebo trvalé (remember my answer). Dajte si záležať, aby ste vybrali jednorazové povolenie (a pri obnove súboru opäť).

1.2.4. Scam

Som 18 ročná dcéra zvrhnutého nigérijského kráľa. Po tom, čo povstalci môjho otca brutálne zavraždili, podarilo sa mi len tak-tak utiecť. O podrobnostiach prevrate sa môžete dočítať na stránkach: (vymenované stránky podobné stránkam CNN, CIA, EU a pod.).

V súčasnosti sa ukrývam a chcem sa dostať do Európy, kde sa chcem dožadovať spravodlivosti. Bohužiaľ na to nemám prostriedky v hotovosti. Otec mi síce zanechal svoje kontá vo Švajčiarsku, na ktorých je stotrinásť miliónov (113 000 000) dolárov. Z miesta v Afrike, kde sa ukrývam, k nim nemám ale prístup.

Ak mi chcete pomôcť a pošlete mi prosím Vás 10 000 dolárov, na zaplatenie miestnych prevádzačov a na moju cestu do Európy. Je to jediný spôsob ako mi zachrániť život.

Za tento šľachetný čin Vás odmením čiastkou rovnajúcou sa 20% z fondov, ktoré mi zanechal môj nebohý otec. To je dvadsaťdva miliónov šesťstotisíc (22 600 000) dolárov.

Tak to je ukážka scamu, takzvaných nigérijských listov[21], ktorý pripravil tisíce ľudí o peniaze a niektorých aj o život.

Ak ste duša romantická, dôverčivá (skôr naivná) alebo ziskuchtivá, tak máte možnosť vykonať šľachetný čin, získať polovicu (časť) kráľovstva a možno (ak ste muž) oženiť sa s princeznou.

[20] Je veľmi vhodné si v takýchto prípadoch pôvodný súbor niekam skopírovať, pre prípad, že by ste ho nevedeli dať do pôvodného stavu.

[21] Scam ale nemusí mať nič spoločné s Nigériou.

Toľkokrát Vám o tom rodičia rozprávali pred spaním. O odvážnych a šľachetných činoch, ktoré boli nakoniec odmenené. A teraz máte na dosah možnosť vykonať takýto čin práve VY. To je niečo, čo sa doteraz dialo iba v rozprávkach. Teraz máte tú možnosť a viete, že sa už nikdy nezopakuje. (Nie je to podvod?) Toľko peňazí. Úbohé dievča.

Ak dostanete scam a neviete o čo ide, určite Vás napadnú myšlienky, nie nepodobné tým z predchádzajúceho odseku. Na formuláciu takých podvodov sa používajú prvky sociálneho inžinierstva. Aj scam Vás chváli – robí z Vás záchrancu, šľachetného človeka. A túto šľachetnosť štedro podporuje dolármi.

Obete, ktoré peniaze poslali, sa slávy samozrejme nedočkali. Možno publicity. Stali sa prípady, že keď sa dožadovali vrátenia peňazí či odmeny, boli pozvaní do Nigérie (alebo iného štátu) dojednať podmienky transakcie. Ak tam šli, boli unesení kvôli výkupnému a prípadne zavraždení. Mnohí spáchali samovraždu, keď prišli o všetky peniaze alebo sa kvôli vidine zisku zadlžili. V roku 2003 si iný druh publicity vyslúžil podvedený muž, ktorý po tom, čo sa zadĺžil, zastrelil v Prahe nigérijského konzula.

Ak niekto o peniaze prichádza, tak niekto iný ich väčšinou získava. Hovorí sa, že scam je v Nigérií tretie najziskovejšie odvetvie ekonomiky.

1.2.5. Spam

Spam je nevyžiadaná, neželaná emailová správa obchodného rázu, nevyžiadaná reklama. Spam neškodí priamo[22], škodí svojím množstvom. Odhady sa rôznia ale množstvo spamu v rámci celkovej emailovej komunikácie sa pohybuje sa v rozmedzí 60 až 90 percent.

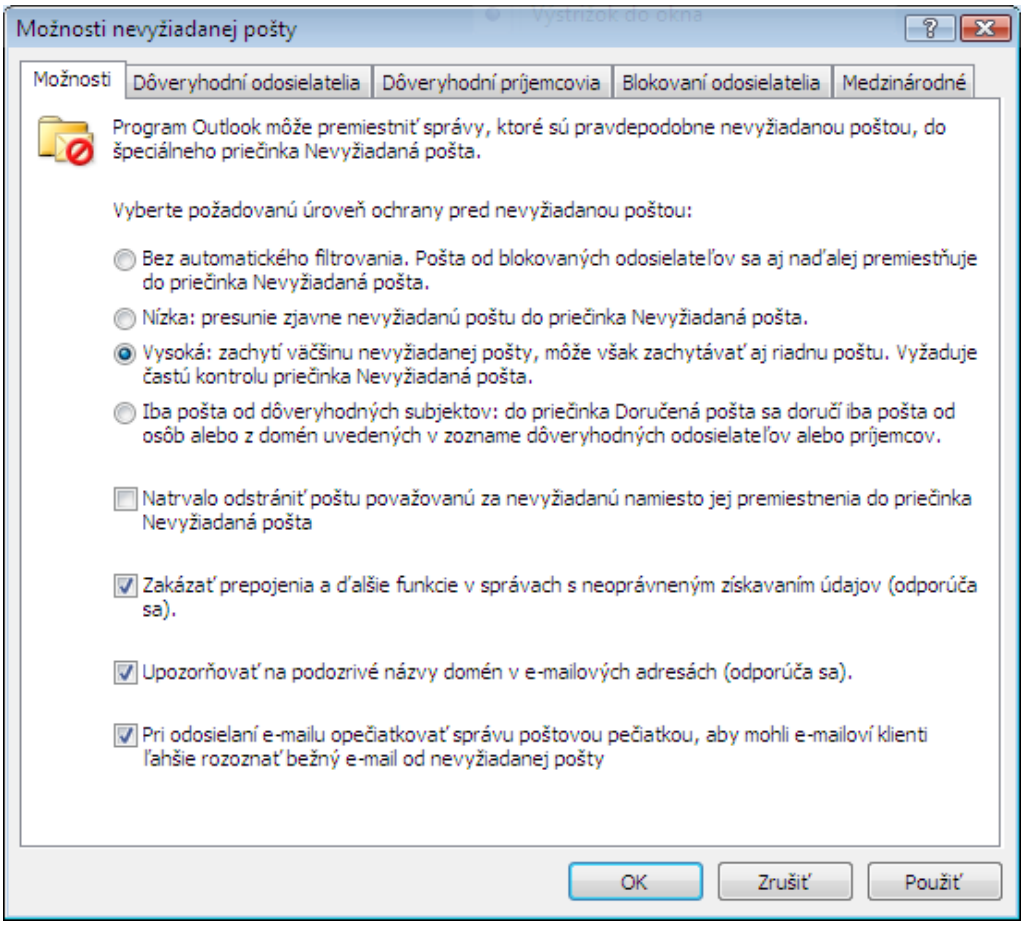
Spam ponúka všetko, o čo môžu mať ľudia záujem. Najčastejšie sú to lieky, prípravky na chudnutie, erotické pomôcky, Viagru a pod.

Na rozdiel od reklamy, ktorú dostávame do klasických poštových schránok, táto reklama spamerov skoro nič nestojí. Aj keď je posielanie emailov lacnejšie ako klasická pošta, pri obrovských množstvách spamu (stámilióny denne) sa už cena môže vyšplhať vysoko. Preto býva lacnejšie najať si hackera alebo tvorcov malware a spam rozosielať z nakazených počítačov bežných používateľov Internetu, ktorí potom nadávajú, „ako ide ten Internet pomaly“.

Spam nie je len nepríjemnosť. Výber a mazanie spamu zaberá zamestnancom čas. Problémom je totiž aj to, že spam môže mať adresu odosielateľa sfalšovanú tak, aby vzbudil väčšiu dôveru. Ak dostanete denne pätnásť spamov a identifikácia jedného trvá dvadsať sekúnd, stratíte päť minút. Málo? Dá sa to podať aj inak, ak je vo firme deväťdesiat zamestnancov, jeden nerobí nič iné len vyraďuje spam. To stojí zamestnávateľa peniaze. Ďalším dôsledkom, ktorý môže nastať je, že pri mazaní kopy spamu sa ľahko omylom zmaže aj dobrý email a to môže viesť taktiež k finančnej strate.

[22] V malej miere sa vyskytuje aj spam obsahujúci malware.

Spam postihuje hlavne firmy a ľudí, ktorí majú svoje emailové adresy vystavené na webových stránkach. Programy spamerov alebo tých, čo im adresy predávajú, prechádzajú po celom Internete, využívajúc odkazy na stránkach, aby prechádzali zo stránky na stránku a zbierajú emailové adresy. Preto sa možno stretnúť s tým, že čoraz viac ľudí má emailovú adresu uvedenú vo forme pochopiteľnej pre človeka ale nezrozumiteľnú pre program. Príkladom takéhoto zápisu je adresa: janka[bodka]pekna[zavináč]zoznam[bodka]sk. Inou možnosťou je mať zobrazenú adresu pomocou obrázka. Text na obrázku je pre človeka bez problémov čitateľný ale počítače si s ním neporadia.



Obr. 1.3. Nastavenie správania sa MS Outlook pri spame

Na ochranu pred spamom sa na poštových serveroch inštalujú antispamové programy, ktoré sa snažia nepustiť spam k adresátovi. Aj poštový klienti využívajú pravidlá pre identifikovanie spamu. Je tu ale nebezpečenstvo, že nesprávne označia za spam email, ktorý so spa-

mom nemá nič spoločné. Preto sa zodpovednosť presúva na používateľa, ktorý si môže vybrať, či chce email označený ako spam rovno zmazať (pomerne riskantné) alebo iba presunúť do zvláštneho priečinka pre nevyžiadanú poštu, kde môže naraz zhodnotiť a prípadne vymazať všetky spamové emaily. Používateľ má (v závislosti od poštového klienta) možnosť nastaviť prísnosť (úroveň) posudzovania emailov. Pri vyššej úrovni ochrany môže častejšie nastať situácia, keď sa dobrý email označí za spam. Pri nižšej úrovni sa skôr medzi dobré emaily dostane spam.

Spameri sa proti detekcii ich výtvorov samozrejme bránia. Ak by rozosielali spamy iba z jedenej alebo niekoľkých IP adries, bolo by ľahké pre poštové servery blokovať všetky emaily z týchto adries. Aj preto spameri využívajú „služby“ bežných používateľov nakazených počítačov.

Na detekciu spamu sa používa aj analýza textu, ktorá pomerne spoľahlivo detekuje či ide o spam alebo nie. Spameri sa bránia tak, že text sa v emaile prakticky nevyskytuje a všetky informácie sú v jednom alebo viacerých obrázkoch. V roku 2007 sa začal používať spam obsahujúci prílohu vo formáte PDF.

Spamer by rád vedel (mal istotu), že adresa, na ktorú posiela email je živá, že na ňu neposiela spam zbytočne. Overiť sa to dá pri zlom nastavení poštového klienta alebo pri neskúsenom používateľovi celkom ľahko. Väčšina poštových klientov umožňuje prijímať poštu vo formáte html – ako web stránku a väčšina je aj tak nastavená. V kóde spamu sa potom nachádza odkaz na obrázok, napríklad www.spamerking.com/images/deffa34.jpg. Ak chce poštový klient zobraziť používateľovi obrázok, musí si tento obrázok vypýtať od servera. A server si to zaznamená.

Pointa je v tom, že každý príjemca má iný názov obrázku (na serveri to je stále jeden a ten istý obrázok) a podľa toho spamer vie, že spam dorazil na miesto určenia a že sa zobrazil v poštovom klientovi[23]. Aj v prípade, že sa zobrazuje e-mail ako obyčajný text alebo je automatické sťahovanie alebo zobrazovanie obrázkov uložených na serveroch zakázané, používateľ niekedy neodolá a klikne na odkaz. Výsledok je rovnaký.

Otázkou, ktorú si mnohí kladú je či sa spam vyplatí. Odhaduje sa, že na spam reaguje jeden z dvoch miliónov adresátov. Tomu sa teda povie malá úspešnosť. Ale pri miliardách spamov denne je to odozva, ktorá svojím množstvom ďaleko predstihuje ostatné formy reklamy. Hranica rentability je vraj niekde pri jednom z dvadsiatich miliónov.

Variantom na spam je spim. Je to analógia spamu vo svete IM (Instant Messaging).

[23] Ak je obrázok posielaný priamo v texte alebo ako príloha – prezradenie o funkčnosti adresy samozrejme nehrozí a obrázok sa môže bez problémov zobraziť.

1.2.6. Pump and Dump

Pump and Dump je postup ako vystrihnutý z učebnice ekonomiky. Zjednodušený scenár vyzerá nasledujúco:

Podvodníci sa zamerajú na nejaké, extrémne lacné akcie, s ktorými sa prakticky neobchoduje. Pri nich sa dá niekoľkými obchodmi cena zvýšiť. Potom príde na rad spam so super ponukou: „Kupujte akcie spoločnosti XY. Plánuje uzavrieť výhodné obchody s firmou YX. Nákup akcií sa oplatí! Budú rásť!“ Nasleduje nákup vyhliadnutých akcií za pôvodnú – nízku cenu. Ceny týchto akcií vzrastú. Ľudia si prečítajú e-mail, pozrú vývoj na burze a vidia – naozaj ceny akcie idú hore. A mnohí **podľahnú vidine zisku** a kupujú akcie za cenu vyššiu ako bola pred pár dňami a aká opäť bude o pár nasledujúcich dní.

Organizátori tejto akcie nakúpili akcie lacno a predali ich, keď boli drahé. Technicky sa dá povedať, že tí ostatní jednoducho iba zle investovali.

Výhodou oproti bežnému spamu (z pohľadu spamerov) je aj skutočnosť, že pri tejto technike netreba uvádzať adresu pre objednanie tovaru – obchod prebieha cez makléra na burze. A tak sa spojitosť so spamerom dokazuje výrazne ťažšie ako pri klasickom spame.

1.2.7. Hoax – poplašná správa

Hoax je e-mail, ktorý na svoje šírenie využíva dôverčivosť ľudí. Šíri sa výhradne ľudským pričinením a preto jediným spôsobom, ako sa pred takouto správou dá brániť, je opatrnosť a osveta. Hoax je možno spoznať na základe troch skutočností:

- Väčšinou sa odvoláva na **dôveryhodnú** osobu alebo firmu („Bill Gates daruje“, „Microsoft varuje", „FBI oznámila").
- „**Varuje**“ pred nejakým (často absurdným) nebezpečenstvom, **dovoláva** sa súcitu s obeťou alebo obeťami nešťastia alebo katastrofy alebo **sľubuje** za každý preposlaný e-mail nejakú čiastku na nejakú nadáciu.
- **Vyzýva** na okamžité preposlanie ďalším ľuďom.

Nasledujúci hoax sa šíril Slovenskom v čase písania tejto knihy (presné znenie):

VAROVANIE !!!!!!! pošli všetkým

Prezídium Policajného zboru odbor dokladov a evidencií por. Ing. [redacted] *tel:* [redacted]

Varovanie od firmy [redacted] **!!**

Prosím, pošlite túto správu každému, kto má prístup k internetu. Môžete dostať na prvý pohľad neškodný e-mail s prezentáciou v Power Pointe pod názvom "Life is beautiful" ("život je krás-

ny"). Pokiaľ ju obdržíte, za žiadnu cenu prezentáciu NEOTVÁRAJTE a okamžite ju vymažte. Pokiaľ ju otvoríte, na vašej obrazovke sa ukáže správa: "It is too late now, your life is no longer beautiful." **("Už je príliš neskoro, teraz váš život už nie je krásny").** *Následne* **STRATÍTE VŠETKO vo vašom PC** *a osoba, ktorá vám toto zaslala, získa prístup k vášmu menu, emailu a heslu. Toto je nový vírus, ktorý vstúpil do obehu v sobotu poobede. AOL už potvrdil, že je to vážne a že antivirové programy nie sú schopné tento vírus zničiť. Vírus bol vyrobený hackerom, ktorý si hovorí "life owner".*

Prosím, pošlite túto správu všetkým vašim priateľom a požiadajte ich, aby ju čo najrýchlejšie poslali ďalej.

Okrem toho, že takéto emaily obťažujú, je aj celkom prozaický dôvod, prečo ich ignorovať. Ak email príde desiatim ľuďom a tí ho prepošlú ďalším desiatim a to sa ešte päťkrát zopakuje, tak je to vyše milióna e-mailov. To je dosť veľa na takú hlúposť. Ako by spamu nebolo dosť.

Niektorí autori uvádzajú, že takýmto spôsobom zbierajú spameri e-mailové adresy. To zrejme nebude celkom pravda. Aj keď sa pri preposlaní e-mailu adresy zachovávajú, v našom prípade je to iba 60 adries v každom z e-mailov v poslednej vlne (každý pridá desať adries). To je veľmi málo pre spamera, ktorý rozosiela milióny e-mailov. Otázne je aj to, ako by sa spamer k tým e-mailom s adresami dostal.

Asi najlepšou reakciou ako sa zachovať, keď dostanete hoax, je odpovedať tomu, od koho ste ho dostali, že sa stal obeťou poplašnej správy – hoaxu. A že si o tom, čo to hoax je môže prečítať na celkom dobrom serveri hoax.cz.

1.3. Prečo existuje malware

Kedysi bolo obľúbenou témou rozoberať prečo a kto tvorí vírusy. Najčastejšou odpoveďou bolo: niekto si chce dokázať, že to dokáže; niekto sa chce pomstiť; prípadne absurdné alebo paranoidné tvrdenie, že samotné antivírusové spoločnosti, aby mali dôvod existovať a podobne. Peniaze sa pred nejakými desiatimi rokmi neuvádzali.

Dnes by odpoveď jednou vetou znela: Malware existuje hlavne preto, že prináša zisk.

Podľa analýzy Sources of Emerging Cybersecurity Threats, ktorú v roku 2006 pre vládu USA vypracovala vládna agentúra GAO[24] vyplýva, že malware alebo podvodné praktiky využívajú:

- Teroristi, ktorí môžu využívať phishing, scam, spyware alebo iný malware k získavaniu prostriedkov alebo citlivých informácií.

[24] http://www.gao.gov/new.items/d06811.pdf

- Kriminálne gangy. Zvyšuje sa použitie počítačových prienikov organizovanými kriminálnymi skupinami s cieľom obohatenia sa alebo odcudzenia identity.
- Zahraničné spravodajské služby, ktoré používajú niektoré nástroje typu malware na zhromažďovanie informácií alebo priamo na špionážne aktivity.
- Hackeri sa niekedy vlámu do počítačových systémov len pre vzrušenie alebo uznanie v hackerskej komunite. Aj keď si nabúranie sa do vzdialených systémov vyžaduje pomerne veľa skúseností a počítačových vedomostí, hackeri si teraz môžu stiahnuť z Internetu útočné nástroje a tie spustiť proti ich obeti. Tak ako sa stávajú tieto nástroje sofistikovanejšie je ich použitie čoraz ľahšie.
- Vnútorní zamestnanci. Nespokojní zamestnanci môžu byť primárnym zdrojom počítačovej kriminality – nemusia mať veľké počítačové znalosti, pretože ich znalosť cieľového systému im umožňuje získať prístup do tej časti systému, kde môžu dáta zničiť alebo ukradnúť. Do tejto skupiny patria aj zamestnanci outsourcingových spoločností. Zamestnanci, ktorí iba náhodou umožnia vstup malware do systému (napríklad svojou neodbornosťou) patria do tejto skupiny tiež.
- Operátori botnet, sú to hackeri ale namiesto pre súťaženie alebo uznanie, ovládnu množstvo systémov s cieľom koordinovane útočiť a distribuovať malware, spam, scam a phishing. Služby týchto sietí sú často na predaj na čiernych trhoch.
- Phisheri sú jednotlivci alebo malé skupiny snažiace sa získať informácie vedúce k peniazom.
- Spameri sú jednotlivci alebo organizácie distribuujúce nevyžiadaný e-mail so skrytou alebo falošnou informáciou so zámerom predať produkty a tiež distribuovať spyware alebo malware.

Podľa spoločnosti Kaspersky[25] sa delia tvorcovia malware na dve skupiny kybervandalov a ozajstných programátorov. Každá zo skupín sa delí na dve podskupiny.

Kyber-vandali, prvá úroveň – v minulosti väčšinu malware vytvorili mladí programátori, deti, čo sa ledva naučili programovať a chceli si otestovať svoje schopnosti. Väčšina

[25] http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280553

ich výtvorov sa našťastie nerozšírila, zanikla spolu s dátami na preformátovaných diskoch. Malware nebol písaný s nejakým konkrétnym cieľom, iba si chceli dokázať, že to zvládnu.

Kyber-vandali, druhá úroveň (script kiddies) – podobne ako prvá úroveň nemajú veľké schopnosti písať malware ale využitím internetu sa napríklad dostanú k hotovým nástrojom alebo k zdrojovým kódom malware, ktorý upravia a púšťajú do sveta, najčastejšie so zámerom ničiť.

Skupina profesionálnych tvorcov malware – Vytvárajú malware pre podsvetie. Sú to tí, z predchádzajúcich skupín, ktorých neopustilo nadšenie pre tvorbu malware a túto tvorbu zvládajú excelentne. Používajú inovatívne postupy, skúmajú softvérové zraniteľnosti a používajú sociálne inžinierstvo originálnymi spôsobmi, aby ich programy nielen prežili ale sa aj čo najviac rozšírili.

Výskumníci - Títo autori majú rovnako ako predchádzajúca skupina záľubu v tvorbe malware a sú rovnako schopní, ale na rozdiel od nej sa nevydali temnou cestou. Sú to obyčajne oni, ktorí nájdu bezpečnostné chyby. Tiež hľadajú nové postupy ako vytvoriť, čo najlepší, nedetekovateľný a najškodlivejší malware.

Keď sa im to podarí, napríklad vytvoria vírus, ktorý nechytá žiadny antivírus pošlú vzorku spoločnostiam, ktoré vyrábajú antivírusové programy. Tie nový vírus preskúmajú, upravia svoj produkt (antivírusový program), tak aby tento vírus (a prípadne aj jemu podobné) detekoval a nový vírus založia „do šuplíka“. V šuplíku je taká vírusová ZOO a vírusy v nej sa aj podľa toho volajú **ZOO vírusy**. Drvivá väčšina existujúcich vírusov sa nikdy neocitla na počítačovej slobode.

Ak nájdu nový postup ako sa dostať do počítača (nájdu chybu v operačnom systéme alebo nejakej aplikácii), často publikujú takzvaný **proof of concept** (dôkaz, že to ide, že myšlienka, postup je správny). Tým upozornia a dokážu, že operačný systém alebo aplikácia je zraniteľná a nemožno ho alebo ju používať nejakým spôsobom. To ale umožní profesionálnym tvorcom (a nielen im) z proof of concept, vybrať to podstatné a využiť to vo svojich kódoch. Problém nastane, ak sa im to podarí skôr ako spoločnosť vyrábajúca zraniteľnú aplikáciu vydá opravu (patch, záplatu) alebo novú verziu. Aj keď sa im to nepodarí skôr a záplata je na už na svete, vždy sa nájde dosť počítačov, ktoré nemajú danú aplikáciu či operačný systém aktualizovaný.

1.4. Ochrana pred malware

Tak ako sa rôznia jednotlivé druhy malware, tak sa odlišujú aj programy, ktoré nás pred nimi chránia. V tejto kapitole je zoznam typov programov, ktoré by nemali chýbať v žiadnom počítači.

1.4.1. Antivírusový program

Antivírusový softvér je asi prvý program, ktorý by si používateľ mal nainštalovať po nainštalovaní operačného systému. Čo sa týka ochranných programov, je antivírus najčastejšie inštalovaným programom. Ale aj tak sa stále nájde dosť počítačov, na ktorých chýba alebo, čo je častejšie, sa ich majiteľ uspokojí s jeho nainštalovaním ale zabúda na jeho pravidelnú aktualizáciu.

Pritom spoločnosti vyrábajúce antivírusové programy niekedy vydávajú aktualizácie aj niekoľkokrát denne. Preto nie je žiadna zbytočnosť nastaviť, aby sa antivírusový program aktualizoval, napríklad, každú hodinu. Presnejšie povedané, aby sa pokúšal aktualizovať, pretože to znamená, že sa iba obráti na server výrobcu s otázkou či je nová verzia alebo aktualizácie. Ak nie je nič nové, tak sa žiadna ďalšia činnosť nevykoná.

Antivírusový program poskytuje minimálne dva spôsoby kontroly. Buď beží na pozadí a dáva pozor na všetky potenciálne nebezpečné aktivity iných programov alebo jeho možné spustiť, aby skontroloval celý počítač alebo vybrané disky či súbory.

Antivírus by nemal byť spúšťaný len občas – keď sa nám niečo nezdá. Mal by sa spúšťať automaticky so štartom operačného systému a byť aktívny po celú dobu používania počítača. Tak má väčšiu možnosť zachytiť vírus (niektoré antivírusové produkty dokážu detekovať aj niektoré iné druhy malware) a takto predísť infekcii a jej prípadnému zamaskovaniu, napríklad rootkitom.

V počítači môže v jednom momente správne fungovať iba jeden antivírusový program. Čo ale neznamená, že ich nemôžete mať nainštalovaných viac. Je ale nutné zabezpečiť, aby sa pri štarte spustil iba jeden. V prípade pochybností (a pri malware nie je žiadna paranoia dostatočne veľká) možno aktívny antivírus vypnúť a dať skontrolovať systém druhým. Je to z dôvodu, že žiadny (antivírusový) program nie je dokonalý. Niektoré sú lepšie pri hľadaní pomocou vzoriek, iné v proaktívnom skúmaní súborov (pozri kapitolu 1.1.1).

Pri výbere antivírusového produktu býva okrem detekcie a odstraňovania vírusov zohľadňovaná aj záťaž systému (testovanie samozrejme zaberá prostriedky počítača) a samozrejme cena.

Porovnania antivírusových produktov bývajú uverejňované na Internete a aj v rôznych počítačových časopisoch. Existujú spoločnosti, venujúce sa porovnávaniu antivírusových produktov.

Najpopulárnejšie antivírusové programy u nás sú NOD32, AVG, Symantec, Kaspersky. Ich využite stojí okolo tisíc korún ročne. Všetky existujú v bezplatnej verzii na skúšobnú dobu.

1.4.2. Firewall

Firewall (protipožiarna stena, možno sa stretnúť aj prekladom ohnivá stena) na rozdiel od antivírusového programu nepozná príliš veľa ľudí. Je to ale program, bez ktorého by sa nemal počítač na Internet a ani na lokálnu sieť pripájať.

Firewall je program, ktorý oddeľuje programy bežiace v počítači od hackerov a červov[26]. V počítači beží viacero programov, ktoré sú schopné a niektoré aj ochotné komunikovať s inými programami po sieti. Tieto programy môžu obsahovať zneužiteľnú chybu v dôsledku chyby v programe (pozri kapitolu 1.1.3). Alebo môžu mať (chybou používateľa) nastavenú slabú úroveň zabezpečenia. Napríklad používateľ nezmenil prednastavené heslo v aplikácii a preto sa môže pripojiť hocikto alebo sú po nainštalovaní operačného systému aktivované sieťové programy, o ktorých ani používateľ netuší, že existujú a preto ich ani nevypne.

Firewall kontroluje požiadavky prichádzajúce po sieti do počítača. Firewall môže upozorňovať aj na programy v počítači pokúšajúce sa komunikovať cez sieť, teda opačným smerom. To je veľké plus k antivírusovému programu, ktorý nemusí zachytiť infekciu a nakazený program sa takto prezradí svojím pokusom komunikovať cez sieť.

V MS Windows XP je zabudovaný firewall ale kontroluje iba smer z Internetu do počítača. V MS Windows Vista je obojsmerný firewall ale kontrola odchádzajúcej komunikácie je po nainštalovaní vypnutá.

Používanie firewallu nie je na rozdiel od antivírusového programu úplne triviálne. To je dôvodom, že používatelia, po tom čo si ho nainštalovali, ho radšej odinštalujú lebo im nejde nejaká sieťová hra, komunikačný program a pod. Druhá a zrejme horšia možnosť je, keď ho nastavia zle a žijú vo falošnej domnienke, že sú chránení. V nasledujúcej časti je načrtnutý postup nastavenia firewallu.

Po nainštalovaní firewall blokuje (skoro) všetku komunikáciu. Ak chce nejaký program komunikovať cez sieť alebo do počítača prichádza niečo zo siete, tak sa firewall opýta používateľa, či má povoliť komunikáciu alebo nie. Tu sa schovávajú dva najväčšie „problémy“ súvisiace s firewallom. Prvým je, že zo začiatku firewall v jednom kuse „otravuje“ so žiadosťami o povolenie alebo zakázanie komunikácie. Druhým je samotná otázka firewallu – ako na ňu odpovedať.

Tieto dva faktory sú často ďalšou príčinou (okrem nefunkčnosti nejakého sieťového programu), ktorá rýchlo vedie k odinštalovaniu alebo vypnutiu firewallu – s odôvodnením, že si ho nainštalujú až vtedy, keď sa bude správať slušne ako antivírus.

---

[26] Tento druh sa nazýva personálnym firewallom. Firewall ale môže chrániť celú sieť pred nepovoleným prístupom z Internetu alebo pred prístupom naň. Vo všeobecnosti oddeľuje navzájom od seba dve siete. V takomto prípade sa nachádza v bode (ako program alebo špecializovaný hardvér), cez ktorý prechádza celá komunikácia medzi týmito sieťami.

Treba sa na to pozrieť z druhej strany. Antivírusový program vie, že keď nájde vírus, tak má konať, ak nenájde, tak nemá obťažovať. Bohužiaľ firewall väčšinou nemôže vedieť, že program, ktorý komunikuje s niekým po sieti je zlý, preto sa pýta. Je na používateľovi, aby premýšľal či má jeho nový šetrič obrazovky dôvod komunikovať s nejakým serverom na Internete.

Aj keď má firewall zo začiatku otázok ako malé dieťa, môže sa rovnako ako deti rýchlo učiť. Okrem odpovede povoliť/nepovoliť je možné vybrať si možnosť povoliť alebo nepovoliť a zapamätať si odpoveď. Firewall sa v takom prípade už nabudúce nespýta a zariadi sa podľa predchádzajúcej odpovede. Firewall samozrejme umožní prezrieť si predchádzajúce zapamätané odpovede a prípadne ich upraviť či odstrániť.

Podobne ako antivírus aj firewall môže byť spustený iba jeden.

Najobľúbenejšie firewaly sú Comodo, Kerio, ZoneAlarm, ktoré sú pre nekomerčné použite zadarmo. Comodo je zadarmo úplne.

1.4.3. Antispyware, antiadware

Aj keď antivírusové programy môžu zachytiť aj iný malware ako vírusy, je možné používať ako prevenciu proti spyware a adware aj špecializovaný program. Mnohé fungujú, podobne ako antivírusy: na pozadí alebo ich je možné spustiť aby skontrolovali celý počítač. Podobne ako firewall (ak fungujú na pozadí) sem-tam položia otázku či povoliť alebo nepovoliť nejakú operáciu. Najčastejšie ide o zápis do registrov alebo do nejakého dôležitého súboru.

Medzi najpopulárnejšie patria Ad-aware, SpyBot SD, Boclean. Všetky tri sú bezplatné (minimálne pre komerčné použitie). MS Windows má zabudovaný Windows Defender.

1.4.4. Aktualizácie

Aktualizácia je proces, pri ktorom sa nahradzujú programy alebo ich časti, ak v nich bola opravená chyba. V prípade ochranných programov okrem toho môže ísť aj o zvýšenie ich účinnosti.

Aktualizovať treba pravidelne, často a automaticky.

Na Internete stále prežíva malware využívajúci chyby, ktoré boli opravené výrobcom softvéru pred niekoľkými rokmi a navyše ho bezpečnostný softvér dokáže detekovať a odstrániť. Prežíva z dôvodu neaktuálnosti systémov a bezpečnostných programov.

Dôvodom neaktuálnosti, býva neznalosť ale často používanie nelegálnych kópií, čo môže znemožňovať aktualizáciu. Crack môže popri odblokovaní programu aj znemožniť jeho aktualizáciu. Autor cracku už len čaká, kým niekto nenájde bezpečnostnú chybu a on ju potom pohodlne využije.

1.4.5. Ochrana všeobecne

Nikdy nepoužite pri spame voľbu unsubscribe (odhlásiť odber), ktorá by mala zastaviť posielanie spamu. Jediným dôsledkom bude potvrdenie, že Vaša e-mailová adresa je živá a budete dostávať ešte viac e-mailov. Niektoré servery pri registrácii vyžadujú e-mailovú adresu. Pre takéto servery si zriaďte osobitnú adresu, určite sa vyhnete množstvu spamu na svojej bežnej adrese.

Nevyužívajte možnosť ukladať alebo zapamätať si prihlasovacie údaje v internetových prehliadačoch. Môže ich zistiť nielen spyware ale aj každá osoba majúca prístup k danému počítaču. Okrem toho si ich opätovným zadávaním trénujete pamäť a pri použití iného počítača alebo prehliadača sa môžete vyhnúť problémom s ich zisťovaním.

Používajte pre rôzne prístupy rôzne prihlasovacie údaje – teda nielen rôzne heslá ale aj rôzne prihlasovacie mená. Aj keď to je zaťažujúce, pri vyzradení jedného prístupu sú ostatné v bezpečí. Heslá si raz za čas zmeňte. Je lepšie, ak je heslo dlhšie a obsahuje veľké aj malé písmená, číslice a prípadne iné znaky.

Venujte pozornosť spôsobu zobrazovaniu prípon. Často sa možno stretnúť s e-mailovou prílohou typu supervideo.mpg.exe. Windows štandardne nezobrazuje prípony známych typov súborov, a tak sa zobrazí iba supervideo.mpg, čo samozrejme nevyzerá nebezpečne.

Pokiaľ Vás napadne nainštalovať si nejaký ochranný program, tak je dobre. Treba si dať ale pozor pri ich výbere. Množstvo spyware a adware sa vydáva za programy, ktoré umožňujú ich vyhľadanie a odstránenie. Vždy nájdu v počítači nejaký malware a obťažujú používateľa s ponukou predaja programu na jeho odstránenie. Ich odinštalovanie je pri tom pre väčšinu takto postihnutých nezvládnuteľný problém. Preto je najlepšie dať na radu uverejnenú v niektorom počítačovom časopise alebo serverov, o ktorých serióznosti ste presvedčený.

Dáta si pravidelne zálohujte. Aj keď o dáta prídete pri nákaze malware málokedy, pre väčšinu ľudí je jednoduchšie a rýchlejšie preinštalovať celý operačný systém ako sa trápiť s odstraňovaním nechcených programov.

1.5. Záver - budúcnosť malware

Ťažko predpokladať, že by sa malware dal na ústup. Ako v každej inej sfére, ktorá prináša zisk sa aj tu budú hľadať nové prístupy. Začínajú sa a naďalej sa budú používať cielené útoky voči jednotlivým firmám s cieľom ukradnúť tajné informácie. Nemožno vylúčiť teroristické kyber-útoky na obranné systémy.

Jednou z tých novších techník je získavanie peňazí z virtuálnych svetov. Príklad ako sa to deje je uvedený v nasledujúcich odsekoch.

Hra World of Warcraft mala v decembri 2006 osem miliónov hráčov. Aj keď je v nej, tak ako vo väčšine virtuálnych svetov zakázané predávanie virtuálnych predmetov za reálne

peniaze (za virtuálne peniaze sa obchoduje priamo vo virtuálnom svete), nie je možné zakázať ich darovanie. A tak vznikli servery ponúkajúce na predaj (za ozajstné doláre) predmety z virtuálnych svetov. Zaplatíte a vo virtuálnom svete dostanete tovar ako dar. Niektorí hráči si takto môžu prilepšovať - sú vo virtuálnom svete dobrí, a tak nemajú problém získať niečo, po čom niekto túži.

Možnosť zárobku využívajú aj podvodníci, ktorí pomocou rôzneho malware získajú prístup k virtuálnej postave a okradnú ju. Tieto veci potom predajú na už uvedených serveroch. Je to pomerne ľahký zárobok, pretože hráčmi sú vo väčšine prípadov deti, ktoré (napriek tomu, že v nich rodičia a starí rodičia vidia počítačových géniov) nemajú často ani potuchy o počítačovej bezpečnosti.

Na takejto situácii je **úsmevná** predstava ako podávate na súde žalobu na neznámeho páchateľa, ktorý Vás okradol o elixír umožňujúci dýchať pod vodou, prsteň 20% rezistencie voči ohňovej mágii a obojručný meč s drainlife 10%[27]. Na krádeže vo virtuálnom svete zatiaľ neexistujú zákony, a tak sú páchatelia stíhaní za činnosti s tým súvisiace, najčastejšie za hacking. Spolu s World of Warcraft je z virtuálnych svetov najčastejším cieľom takýchto útokov Lineage.

Nastupujúcim trendom je malware špeciálne určený pre mobilné telefóny a PDA. Aj keď sa už niekoľko rokov vyskytujú, ich skutočný boom nastáva práve teraz. Ceny takýchto zariadení klesajú a stávajú sa tak prístupné najširším vrstvám. Počítačoví používatelia majú aké-také povedomie o bezpečnosti. To sa ale nedá povedať o každom, kto bude v blízkej dobe využívať mobilný telefón.

Obľúbeným rozšírením funkcionality prehliadačov sú takzvané doplnky (add-on). Tie sú a v budúcnosti budú tiež cieľom útokov hackerov [28] alebo priamo ich výtvorom. V prípade ich vytvorenia hackerom si netreba predstavovať, že doplnok robí nejakú škodlivú činnosť – to by bolo priehľadné. Pravdepodobnejšie je, že to bude užitočný doplnok, ktorý si nainštaluje mnoho ľudí. Bude ale obsahovať zneužiteľnú chybu - on alebo jeho niektorá vylepšená verzia.

Obdobným spôsobom môže hackerská alebo teroristická skupina založiť firmu vyvíjajúcu napríklad firewall. Firewall bude zadarmo, bude dobrý (kto iný tomu môže lepšie rozumieť?). Ideálne je ak firma začne vyrábať aj antivírusový a antispyware program. Balík týchto bezpečnostných programov sa rýchlo rozšíri, budú ho používať milióny ľudí. Budú ho chváliť aj renomovaní odborníci. A potom príde nová verzia...

[27] Majiteľovi vylieči 10% života, z každého ním spôsobeného zranenia.

[28] Nárast bezpečnostných chýb v doplnkoch dokumentuje Symantec nasledujúcimi počtami: 34 v prvej polovici 2006, 74 v druhej polovici 2006 a 237 v prvej polovici 2007.