UNIVERZITA PALACKÉHO V OLOMOUCI
PEDAGOGICKÁ FAKULTA
Katedra technické a informační výchovy

Bakalářská práce

Ladislav Orel
Informační výchova se zaměřením na vzdělávání a geografie

Problematika malware a znalost škodlivého kódu u žáků základních škol

Olomouc 2016 Vedoucí práce: doc. PhDr. Miroslav Chráska, Ph.D

Čestné prohlášení

Svým podpisem zde stvrzuji, že bakalářskou práci: „Problematika malware a znalost škodlivého kódu u žáků základních škol.“ jsem vypracoval samostatně. Veškeré použité materiály a podklady, ze kterých byly čerpány informace, jsou uvedeny v seznamu použité literatury a jsou řádně ocitovány dle citační normy ČSN ISO 690.

V Olomouci dne 18.4.2016 ……………………………….

Ladislav Orel

Poděkování

Rád bych zde uvedl člověka, jenž byl vedoucím moji bakalářské práce – doc. PhDr. Miroslav Chráska, Ph.D. Poskytl mi pomoc a cenné rady v době, kdy byla tato práce vytvářená. Taktéž bych zde rád uvedl člověka, který sice neví, že tato práce vznikala, ale o této problematice hodně ví, již od mala se ji věnoval a vytvořil web www.viry.cz, ten člověk se jmenuje Igor Hák, o problematice malware píše jak odborné, tak populárně naučné články a vede mnoho seminářů, i z jeho bakalářské práce a webu byly čerpány informace do této práce. Poděkování patří také mojí přítelkyni. V době tvorby této práce mi moc pomáhala a morálně mě podporovala.

Obsah

Úvod

S technickým pokrokem přicházejí i nové možnosti v oblasti informačních a komunikačních technologií, kde je také tento proces znát nejvíce. Technika jde stále rychleji a více kupředu. Bylo zjištěno, že se práce dá usnadnit technickými vymoženostmi. Začalo to tím, že matematické problémy byly řešeny jednoduchými kalkulátory, byly vyvinuty dírkové systémy, velké sálové počítače apod. Nové možnosti však přináší i řadu nevýhod. Pokud je možnost zařízení určitým způsobem naprogramovat, může se objevit i někdo, kdo této skutečnosti zneužije a naprogramuje jej tak, aby práci neulehčil, ale naopak znepříjemnil nebo znesnadnil. Vždy se najde někdo, kdo bude chtít některé produkty zničit, znehodnotit, rozbít. Ve virtuálním světě ICT[1] se tato problematika nazývá malware. Primárním cílem malwaru je poškodit technická zařízení. Zpočátku šlo o jednoduché triky programátorů - jednalo se pouze o žerty, ale s postupem času se veškerý malware stává stále více sofistikovaným a mnoho tvůrců jej tvoří spíše pro vlastní zisk, než pro zábavu. Na druhou stranu existují i antivirové společnosti zabývající se naopak tím, jak se malwaru zbavit. Tato bakalářská práce se zabývá právě problematikou malwaru, včetně jeho rozdělení i způsoby prevence a ochrany.

Bakalářská práce: „Problematika malware a znalost škodlivého kódu u žáků základních škol.“ je rozdělena do 2 částí - teoretické a praktické.

V teoretické části jsou popisovány širší souvislosti pojmu malware. Přes krátké uvedení pojmu je zde ve stručnosti nastíněna historie problematiky malware a její vývoj, různé druhy škodlivého kódu včetně variací a rozčlenění. Zmíněny jsou i slavné škodlivé kódy, které způsobily nemalé škody a mezi lidmi vzbudily obecný zájem. Teoretická část je zakončena kapitolou o prevenci před škodlivým kódem.

Rychle vyvíjející se technologie si žádají odlišný přístup ve vzdělávací oblasti informační a komunikační technologie. Na základních školách by žáci mohli být lépe seznámeni s novými typy technologií. Bylo by na místě, aby byli informování o možných rizicích technického pokroku, které jsou spojeny s novými vymožeností a jejich používáním. Lepší znalost povede k lepší orientaci a větší obezřetností mladých lidí v kyberprostoru. Praktická část je proto věnována výzkumu znalosti škodlivého kódu u žáků základních škol. Je zde popsána metoda výzkumu, jsou formulovány hypotézy a výzkumné předpoklady. Následně jsou analyzována a vyhodnocena data a na konci výzkumné části jsou pak diskutovány výsledky, z nichž vyvozuji patřičné závěry.

[1] ICT – zkratka pro informační a komunikační technologie

1 Cíle práce

1.1 Cíl teoretické části

Cílem teoretické části podat a popsat informace související s problematikou malware. Základní znalost škodlivého kódu je dnes takřka nutností, většina technických zařízení je již na takové úrovni, že existuje mnoho možností, jak zařízení napadnout. V lepším případě půjde jenom o ztrátu dat nebo poškození softwarové[2] části systému, v horším případě pak ztráta finančního obnosu z bankovního účtu nebo hardwarové[3] poškození[4] části přístroje. V práci je popsána problematika malwaru a pojmy s ní související, členění škodlivého kódu, možnosti ochrany proti škodlivému kódu a vývoj malwaru.

1.2 Cíl praktické části

Cílem výzkumné části bakalářské práce, je zjistit, jaké znalosti mají žáci základních škol v oblasti škodlivého kódu (malwaru).

Dílčí cíle výzkumné části BP jsou:

Zjistit, jestli existuje v problematice malware rozdíl mezi znalostmi chlapců a dívek.

Zjistit, zda již byli žáci někdy napadeni škodlivým kódem, a jestli napadení vedlo k doplnění znalostí o této problematice.

Zjistit, jaký je podíl žáků, kteří se považují za technický typ a jestli má tato skutečnost vliv na jejich znalost malwaru a škodlivého kódu.

Zjistit, jestli žáci znají pojem malware pouze obecně, nebo mají znalosti i o jeho členění a zda mají nějakou představu o ochraně před škodlivým kódem.

---

[2] Software – nehmatatelná část počítačů, programové vybavení počítačů – zajišťuje chod systému, programů.

[3] Hardware – hmatatelná/fyzická část přístroje – jednotlivé součástky přístroje.

[4] Poškození hardwaru softwarem – v dnešní době takřka nemožné. Výrobci, kteří vyrábí jakýkoliv hardware, se snaží o to, aby měl hardware nějakou zpětnou vazbu nezávislou na samotném systému, ve kterém se hardware nachází. Hardware pak sám sebe kontroluje a zároveň zabraňuje potencionálnímu nebezpečí, které by hrozilo ze strany softwaru.

Teoretická část

2 Malware

2.1 Úvod do problematiky malware

Malware je obecně škodlivý kód, který obsahuje viry, červy a trojské koně apod. (Trendmicro, nedatováno) a jak už bylo řečeno v úvodu, takto může být označen jakýkoliv škodlivý kód, který není nijak prospěšný a má za úkol v počítačích (či jiných zařízeních) škodit.

Slovo vzniklo spojením 2 anglických slov, tato dvě slova jsou malicious[5] a software, dohromady tedy malware.

Nejpočetnější a nejznámější typ malwaru, který se běžnému uživateli obvykle vybaví, je počítačový virus. Mezi běžnými uživateli často dochází k chybnému chápání pojmů počítačový vir a malware, ty však nejsou synonymní. Malware je nadřazeným pojmem a vir je pouze jedním z různých typů škodlivého kódu. Pod pojem malware se dále mimo viry řadí červy, trojské koně, rootkity, exploity apod. (tyto výrazy budou vysvětleny v dalších kapitolách).

2.2 Definice malware

Pro malware existuje několik definic:

Ministerstvo vnitra ČR definuje malware jako: *„souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty).“* (Ministerstvo vnitra, 2009, s. 2).

Společnost Kaspersky LAB uvádí: *„Slovo malware vzniklo zkrácením anglického sousloví malicious software (škodlivý software) a označuje jakýkoli počítačový program, jehož cílem je provádět nežádoucí činnosti či poškozovat oprávněného uživatele počítače, jakým jste kupříkladu i vy.“* (Kaspersky LAB, 2015).

[5] Z angl. jazyka: malicious = zákeřný → malware volně přeloženo = zákeřný software.

Tvrzení společnosti Cisco říká, že malware je (přeloženo): *„…kód nebo software, který je specificky navržen pro poškození, narušení, ukradnutí, nebo obecně ke způsobení nějaké „špatné“ nebo nelegitimní akce na data, uživatele nebo síť.“* (Cisco, nedat.).

Z předešlých příkladů je na první pohled jasné, že definice malwaru se mohou navzájem lišit, a každý je může popsat odlišně. Co se však neliší, je fakt, že malware je téměř vždy primárně navržen k poškozování a jedná se o nelegální trestnou činnost.

2.3 Malware a jeho vývoj

2.3.1 Creeper jako první malware

Malwarovým průkopníkem je program s názvem Creeper. Jeho první výskyt se datuje na rok 1971. Byl vytvořen jako experiment a nebyl určen k poškozování systémů, jeho činnost byla naprogramována tak, aby pouze zobrazovala zprávu o jeho výskytu v systému: *„I'm the creeper, catch me if you can!“*[6]. Creeper byl schopen sebe-replikace, jednalo se tedy také o prvního červa[7] (HELPNETSECURITY, 2011).

2.3.2 První „antivirový program“ Reaper

Krátce po Creeperovi byl vyvinutý program Reaper. Byl naprogramován tak, že při vniknutí do systému zjišťoval přítomnost Creepera. Pokud byl Creeper nalezen, tak ho Reaper vymazal spolu se sebou samým, pokud Creeper v systému nalezen nebyl, tak se program Reaper vymazal. Reaper byl naprogramován také jako červ, ale ve své podstatě se choval jako první antivirový jednoúčelový program (Szor, 2006).

2.3.3 Klidná 70. léta

Doba 70. let dala vzniknout několika prvním malware programům. Ty však tehdy nebyly určeny přímo k poškozování, šlo o univerzitní experimenty a pokusy v laboratorních podmínkách, kdy nebylo cílem vypustit škodlivý program mimo

[6]Přeloženo do českého jazyka z angl. jazyka: „Jsem Creeper, chyť mě, jestli to dokážeš!“
[7] Červ – typ malwaru schopný množit sám sebe, bude upřesněno v 3. kapitole.

testovanou oblast. Mezi takové můžeme zařadit již zmíněné programy Creeper a Reaper nebo také ANIMAL[8].

2.3.4 Zlom v 80. letech

Přelom, který nastal v 80. letech, přinesl více programů, které byly přímo určeny ke škodě napadeného systému a uživatele. Veřejnost tehdy ještě netušila, že něco jako malware existuje, což napomáhalo tvůrcům malwaru k jeho efektivnějšímu šíření.

Mezi první, více škodlivý malware můžeme zařadit virus Elk Cloner. Elk Cloner byl virus vytvořen v roce 1982 tehdy teprve 15letým studentem. Richard Skrenta tehdy vytvořil Elk Cloner pro počítače značky Apple II původně jako žert. Šlo o boot sector[9] virus, který po úspěšné infekci zařízení při detekci vložených disket nově datová media infikoval. Virus byl už tehdy naprogramován velice chytře, například pokud byla vložená disketa již v minulosti někdy infikována, tak ji virus znovu neinfikoval/nepřepisoval. Infikované prostředí bylo označené speciální „značkou“, podle které virus poznal, že prostředí již bylo infikováno. Přesně po padesátém spuštění počítače nenaběhl systém, ale samotný Elk Cloner, který způsobil neovladatelnost zařízení. (TechTarget, 2005). Další malware, který v 80. letech trápil uživatele, se jmenoval EGABTR, známý také jako EGGBEATER. Byl to program, který falešně sliboval vylepšení výkonu a zobrazování EGA[10] monitorů, nicméně jeho pravá podstata spočívala v tom, že kompletně smazal soubory z disku (BITDEFENDER, 2010).

2.3.5 Obezřetnost v 90. letech

Začátkem 90. let pak malware definitivně vstoupil do povědomí společnosti a uživatelé začali být obezřetní mnohem více než dříve. Bohužel s rostoucím pokrokem techniky přišly i nové možnosti, jak systém napadnout. Mezi takové novinky můžeme řadit polymorfní a stealth viry, což bylo zcela něco nového a nečekaného (pojmy stealth virus a polymorfní virus budou vysvětleny v dalších kapitolách).

---

[8] Program ANIMAL nebyl nebezpečný ani škodlivý, vytvářel pouze složky s názvem zvířat všude, kde měl uživatel povolený přístup se zápisem. Nejednalo o nebezpečí, ale spíše o znepříjemnění používání přístroje.

[9] Boot sector – oblast vytýčena systémem pro spouštění operačního systému. Pokud dojde k její infekci, malware se může přednostně načítat ještě před samotným operačním systémem.

[10] EGA zkr. z angl. jazyka – Enhanced graphic adapter = rozšířený grafický adaptér. EGA byly standardizované počítačové monitory firmy IBM používané od roku 1984. Jsou následovníky monitorů CGA a předchůdci VGA monitorů.

V roce 1988 byl objeven virus Cascade[11], jehož „řádění“ bylo hlavním důvodem pro vytvoření ochrany proti škodlivému kódu. Předchůdce prvního opravdového antivirového programu vznikal ve firmě IBM, nebyl ale určen pro běžné uživatele, ale pouze pro pracovníky firmy IBM (F-secure, nedatováno).

2.4 Současná situace v oblasti působení malwaru

V současné době se malware postupně přesouvá z desktopového prostředí na mobilní zařízení – to však neznamená, že by z počítačů, notebooků a ostatních nepřenosných zařízení zmizel úplně, nicméně masové a velmi časté využití mobilních telefonů s možností okamžitého přístupu k síti využívají vývojáři škodlivého softwaru k napadení těchto zařízení, jelikož je u nich vyšší šance k infekci a je snazší malware rozšířit. Snaha bezprostředně ničit a mazat uživatelská data se mění v kontrolované sledování obětí, cílený marketing (tzv. legální spyware spojený s adwarem), automatické přesměrování na reklamu bez vědomí uživatele, krádeže identit spojené s možným phishingem a šifrování uživatelských dat s příslibem odšifrování po zaplacení výkupného autorům malwaru.

2.5 Vyhlídky do budoucnosti

Jistým způsobem se dá předpokládat, že budoucí směr malware se bude soustředit stále více na přenosná zařízení a sledování veškerého obsahu, který bude možno ze zařízení získat (historie prohlížení internetu, nezašifrovaná uložená hesla k různým účtům, čtení obsahu sms zpráv, čtení seznamu uložených čísel pro rozesílání SPAMu[12] apod.). Skutečnost upřednostňování prohlížení webových stránek skrze mobilní zařízení vyplývá např. z celkové četnosti přihlášení na Facebook[13]. Tato sociální síť zaznamenala enormní nárůst prohlížení Facebooku v roce 2015 skrze mobilní zařízení oproti předešlým rokům a návštěvám této sociální sítě skrze zařízení nepřenosná (Facebook, 2015).

Využití mobilních zařízení pak nemusí být typické pouze pro Facebook, ale i k prohlížení jiných webových portálů. Domnívám se, že tomu tak je proto, že pro

[11] Cascade způsoboval „pád“ textu. Některý text na obrazovce zůstával tam, kde měl a jiný text „popadal“ na spodní stranu obrazovky a zůstal „ležet“ – pády připomínaly padání kostek ze hry Tetris.

[12] SPAM – nevyžádaná pošta. Spam nemusí obsahovat škodlivý software, může pouze způsobovat nepříjemné zahlcení emailové schránky, avšak může obsahovat odkazy na podvodné stránky nebo dokonce i samotný malware.

[13] Facebook.com – oblíbená sociální síť založená na principu mini-blogu a dopisování si s přáteli v reálném čase.

jakéhokoliv uživatele je pohodlné vzít do ruky telefon a brouzdat po internetu v okamžiku, kdy cítí potřebu a nemusí proto zapínat stolní počítač. Pří brouzdání po internetu pak může být neobezřetný nebo nezabezpečený uživatel infikován i na mobilním zařízení.

2.6 Rozdíl Hacker VS Cracker

Člověk, jenž vytváří škodlivý kód je mylně nazýván hackerem, správný název pro takového člověka je výraz cracker[14]. Cracker má v úmyslu něco rozbít, poškodit. Termín hacker naopak označuje člověka se značnými znalostmi v oblasti IT. Hacker se tedy původně snažil „zkáze“ předejít a zařízení ochránit. Za chybné chápání pojmu hacker mohou média, která tímto termínem označovala především tvůrce malwaru a tato konotace pojmu pak vstoupila do povědomí laické veřejnosti (Jagoda, 2015).

2.7 Největší „ryba“ je nejvíce ohrožena

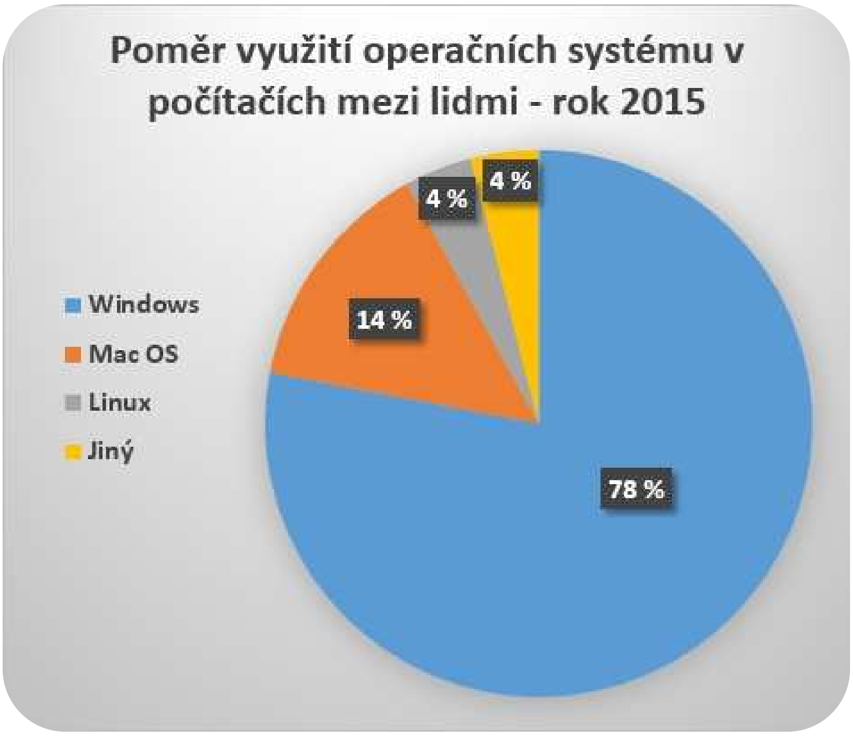
Podstatou malware je poškodit uživatele co nejvíce. To se daří, pokud je malware co nejvíce rozšířen a tohoto rozšíření se nejlépe dosahuje v systémech, které jsou uživateli nejčastěji používány.

Nejvíce užívaným operačním systémem mezi lidmi je systém Windows a jeho odnože (Statista: the statistics portal, 2015). Právě na OS Windows se tvůrci malwaru zaměřují nejvíce. Vezmeme-li například program, který je uzpůsoben škodit v systému Windows, ale v Linuxu[15] nefunguje, je velice pravděpodobné, že když používá 9 lidí z 10 operační systém Windows, tak je šance uchycení takového programu mezi milionem lidí a následné poškození daleko vyšší, než malware fungující v Linuxu, který však ve Windows fungovat nebude a poškozený bude 1 člověk z 10 a to jenom v případě, že se programu podaří proniknout skrze bezpečnostní opatření.

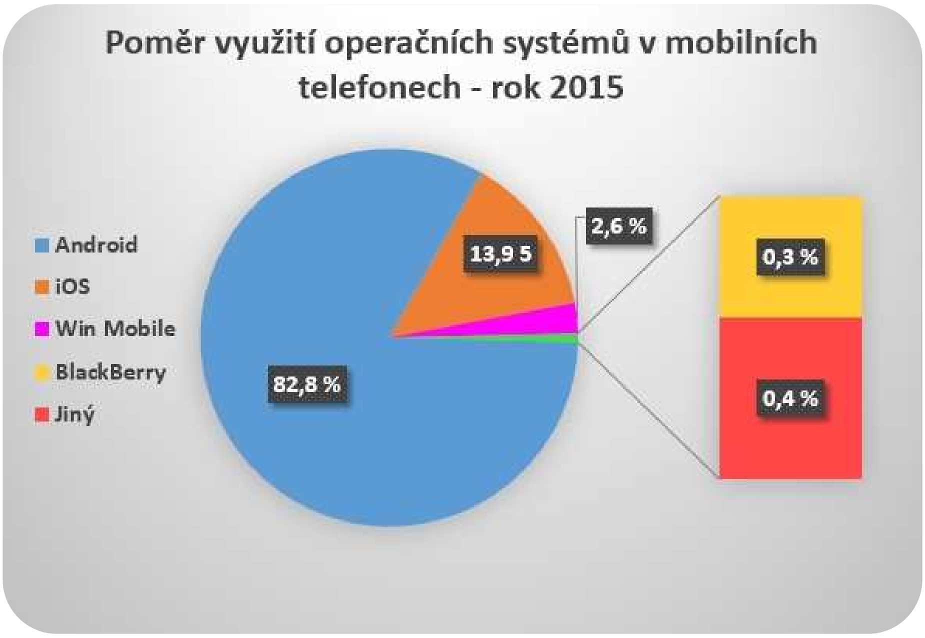
[14] Z angl. jazyka: crack = rozbít. Cracker je člověk, který má v úmyslu něco poškodit nebo zničit pomocí malwaru.

[15] Linux – víceúlohový, víceuživatelský operační systém založený na GNU licenci – licence pro svobodný software tzn. software k použití zdarma.

Podobně je tomu tak u mobilních zařízení, kde se nejvíce mezi lidmi používá v současné době operační systém Android[16] a jeho variace (ICD, 2015). Útok na Android je pak pro tvůrce malwaru výhodnější. Naopak vytváření malwaru např. pro Symbian[17] by byla nejspíše jenom ztráta času, protože tento operační systém se mezi lidmi objevuje velice zřídka.



Graf 1: Poměr využití operačních systémů v počítačích. Zdroj: (Statista: the statistics portal, 2015)



Graf 2: Poměr využití operačních systémů v mobilních telefonech. ZDROJ: (ICD, 2015)

[16] Android – operační systém pro mobilní zařízení založený na Linuxovém jádru.
[17] Symbian – operační systém nejvíce používaný v mobilních telefonech značky Nokia, zřídka i v některých zařízeních značky Sony Ericsson. Tento operační systém je již však takřka „mrtvý“ a používá ho velice málo lidí.

3 Rozdělení malware

3.1 Počítačový virus

rnění
cování.

Asi nejznámějším možným malwarem je počítačový virus, který má mnoho podob a variací. Počítačový virus je škodlivý kód a „právem“ se nazývá virem, protože pracuje na podobném principu, jako virus biologický, kdy v těle hostitele napadá buňky, do kterých vkládá svoji informaci – buňky v těle tedy můžeme chápat jako spustitelné programy v počítači. Počítačový virus má za úkol infikovat uživatelské prostředí a škodit v něm. Virus potřebuje ke svému šíření jiný spustitelný program, do kterého vloží svoji škodlivou informaci. S příštím spuštěním modifikovaného programu se pak vykoná naprogramovaná akce. Virus sám sebe replikovat[18] nemůže, potřebuje k tomu vždy využít jiného prostředí (na rozdíl od tzv. červa, o kterém se bude psát v dalším členění).

Frederick Cohen poprvé definoval virus (přeloženo): *„...jako program, který může infikovat ostatní programy a modifikovat je tak, že obsahují potencionálně vyvinutou kopii sebe samého.“* (Cohen, 1987).

3.1.1 Dělení počítačových virů dle setrvání v paměti

3.1.1.1 Rezidentní virus

Virus se nachází v systému „na pozadí“ a může neustále ovlivňovat činnost systému. Co hraje na jeho stranu je, že může být naprogramován tak, aby sledoval činnost uživatele a napadal přímo soubory, které jsou právě používány a tím zvýšit riziko rozšíření a infekce. (Hák, 2005)

[18] Replikace – vytvoření sebe sama jako kopii.

3.1.1.2 Nerezidentní virus

Virus, který vykoná jednorázově svoji naprogramovanou akci, se následně neukládá do operační paměti. Nerezidentní virus dobře popisuje Igor Hák, který přímo píše: *„Tyto viry nevyužívají paměť pro své šíření. Stačí jim, když jsou aktivovány společně s hostitelským programem. Pak přebírají řízení jako první, provedou svoji činnost, nejčastěji replikaci a předají řízení zpět hostitelskému programu. Replikací zde většinou rozumíme například napadení všech vhodných souborů (postupně nebo naráz) v aktuálním adresáři, či napadení souborů uvedených v proměnné DOS PATH.“* (Hák, 2005, s. 28).

3.1.1.3 Appending virus

Apending, neboli také koncový virus, má za úkol co nejdéle setrvat a držet svoji pozici v infikovaném systému. Je to virus, který se snaží svůj kód vložit na konec programu. Na rozdíl od něj se ostatní viry snaží vkládat informaci hned před spustitelný kód proto, aby se spustily co nejdříve (SANS, 2016).

3.1.1.4 Bootsector virus

Virus, který se snaží infikovat spouštěcí boot sektor. Je to velice zákeřná metoda, a to hlavně proto, že antivirová ochrana je ve většině případech aktivně zapnutá až po naběhnutí samotného operačního systému. Pokud je virus již načtený před samotným operačním systémem, špatně se detekuje a ještě hůř odstraňuje. V případě systému nakaženého boot virem se snaží virus zapisovat i na ostatní přítomná paměťová media (flash disk, externí hard disk apod.) (Kaspersky LAB, 2015).

3.1.2 Dělení dle způsobu detekce

3.1.2.1 Stealth virus

„Stealth[19] *virus je složitý malware, který se po napadení počítače ukryje. Po ukrytí zkopíruje do svého kódu data před napadením, která během vyhledávání virů poskytne antivirovému softwaru. Jedná se tedy (sic!) velice těžko rozpoznatelný a odstranitelný typ viru. …tento typ malwaru je navržen tak, aby se před antiviry aktivně ukrýval. Stealth virus toho docílí dočasným přesunutím z napadeného souboru, zkopírováním svého kódu na*

[19] Z angl. jazyka: stealth = skrytý, schovaný, neviditelný.

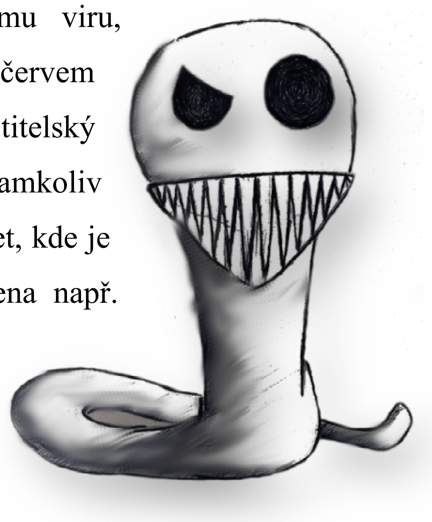
jinou jednotku a nahrazením původního souboru souborem čistým. Tento virus rovněž ve snaze vyhnout se odhalení maskuje velikost napadeného souboru.“ (Kaspersky Lab, 2015).

3.1.2.2 Polymorfní virus

Polymorfní[20] viry jsou programovány tak, aby jejich činnost nebyla detekována uživatelem či antivirem. Dosahují toho tím, že se snaží samy sebe vždy pozměnit. Polymorfní viry fungují na podobném principu jako viry stealth s tím rozdílem, že stealth viry vždy vytváří svoje totožné kopie. Polymorfní viry taktéž vytváří kopie sebe sama, které jsou ale od předešlých kopií zcela odlišné, se zachováním své původní funkce. Virus mění sebe sama užitím různých algoritmů. Nejjednodušší automatický algoritmus, který lze použít, je např. datum a čas, podle kterého by virus měnil svůj kód. (TechTarget, 2007).

3.2 Červ

Červ je varianta velice podobná počítačovému viru, nejedná se však o ten samý pojem. Rozdíl mezi virem a červem je ten, že červ nepotřebuje ke svému šíření žádný hostitelský program. Červ dokáže replikovat sebe samého kamkoliv (diskety, flash paměti, firemní sítě, emaily či celý internet, kde je možnost šíření nejrychlejší), odkud může být dopravena např. jeho kopie nebo on sám (podle naprogramování) do ostatních systémů a počítačů. Pokud síť, počítač nebo jiný systém, systém, kterému chybí bezpečnostní prvky, nebo v nich jsou mezery, obdrží červa, pak má červ otevřené možnosti k dalšímu šíření. Celý proces s cestováním, následná infiltrace a infekce ostatních strojů se opakuje, pokud nebyl naprogramován jinak (Hák, 2005).



3.2.1 Internetový červ

Ke svému šíření do ostatních systémů či počítačů používá síť internetu. Internet jako samotný nakazit nelze, ale lze nakazit počítače či systémy připojené k němu. Červ

[20] Z angl. jazyka: polymorph = proměna, změna.

neinfikuje soubory, ale pakety[21]. Červem infikované datové pakety následně cestují internetem, usadí se pak v systému, kterému chybí bezpečnostní opatření, jsou zastaralá nebo obsahují bezpečnostní díry (Hák, 2005).

3.2.2 Rabbit

Rabbit[22] je červ, který má ve svém kódu naprogramováno to, že sám sebe replikuje, co nejdéle to jde. Výsledkem bývá buď rychlá detekce, nebo úplné zhroucení napadeného systému. Zhroucení je způsobeno totálním zahlcením paměti neustálou sebe-replikací téhož samého červa (Stamp, 2011).

3.2.3 Octopus worm

Pokud se jednotliví červi dostanou do více systémů, mají možnost mezi sebou komunikovat a jsou vhodně naprogramovaní, mohou vzájemně škodit organizovaně. Komplexně se tento celek jeví jako chobotnice - octopus[23] a jednotlivé infikované systémy můžeme chápat jako její chapadla. Je možné se také setkat s podobným případem, kdy se infikovaná síť nazývá „botnet“ a jednotlivé systémy v napadené síti se nazývají tzv. „zombie počítače“[24]. V takovém případě však nejde o organizovanou škodlivou činnost, nýbrž spíše chaotickou, kdy jednotlivé malware prvky způsobují různou činnost nezávisle na ostatních prvcích (SANS, 2002).

3.3 Trojský kůň

Velice podobný viru s tím rozdílem, že není schopen replikovat sám sebe, sám také nemůže infikovat ostatní soubory a nedokáže se šířit a škodit bez pomoci uživatele. Jedná se o samostatný program, nejčastěji typu *.EXE, který vypadá jako neškodný software. Po spuštění však vykoná škodlivou činnost.

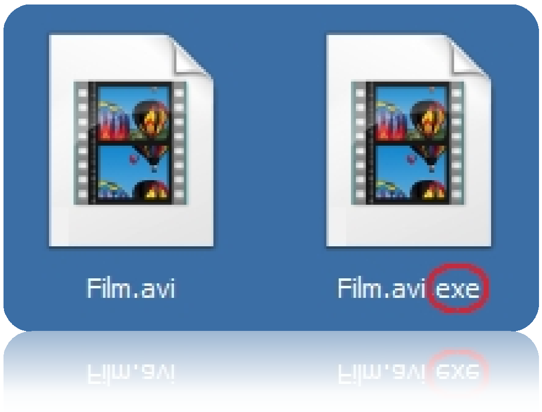
[21] Data, která odchází a přichází z počítačů, jsou uzavřena v tzv. paketech. Paket = malý balíček s informacemi.

[22] Z angl. jazyka: rabbit = králík. Označení rabbit vzniklo na odkaz pohromy v Austrálii, kdy v roce 1859 došlo k přemnožení králíků. Králici zde neměli přirozeného nepřítele a způsobili nemalé škody.

[23] Z angl. jazyka: octopus = chobotnice.

[24] Zombie počítač – infikovaný počítač, který může být na dálku ovládán někým jiným nebo jeho chování ovlivňuje samotný malware např. k rozesílání SPAMu.

Z výše uvedeného faktu je zřejmé, že trojský kůň nemůže infikovat ostatní soubory, a že nepotřebuje žádného hostitele. Trojský kůň je program, který se dá vyléčit pouze smazáním celé aplikace, tzn. ve většině případů celý *.EXE soubor. Velikou nevýhodou je, že samotná aplikace nebo program se může jevit díky ikoně např. jako obrázek, nebo *.MP3 soubor. Většinou jsou totiž trojské koně psány pro systémy Windows, kde je primárně nastavená možnost skrývání přípon souborů známých typů - aplikace *.EXE se škodlivým programem se tedy pro uživatele může jevit jako obrázek nebo písnička, jenom proto, že ikonu tohoto programu si uživatel mylně spojí s prohlížením obrázků nebo přehráváním médií (Hák, 2005).



3.3.1 Password stealing-trojan horse

Je spustitelný soubor, který byl vytvořen za účelem kradení cenných citlivých údajů a informací, nejčastěji přihlašovacích údajů (PIN kódů, hesel k emailům, do internetového bankovnictví apod.). Tento typ programu pracuje tak, že sleduje jednotlivé úhozy kláves, které uživatel stiskne na své klávesnici (tzv. keylogger), a následně je ukládá jako textový soubor, který poté odešle osobě, která chce poškodit dotyčného uživatele zneužitím odcizených informací, např. následným „vloupáním" na jeho bankovní účet. Password Stealing trojan[25] má tedy funkci, podle kterého ho můžeme zařadit mezi „spyware" (Hák, 2005).

3.3.2 Destruktivní trojský kůň

Malware naprogramovaný tak, že jeho jediným cílem je po spuštění zničit nebo znehodnotit co nejvíce uživatelských dat. Nejčastěji maže data, která zrovna disk či uživatel prochází nebo jednoduše zformátuje[26] disk celý (Hák, 2005).

[25] Z angl. jazyka: password = heslo, steal = ukrást →password stealing trojan = trojský kůň navržený pro krádeže hesel.
[26] Formát disku – kompletní vymazání dat z disku.

Tyto programy bývají někdy velice „jednoduché“ a proto nemusí být detekovány antiviry už jen z toho hlediska, že se jejich činnost blízce podobá samotnému požadavku od uživatele (ačkoliv třeba nechtěnému) podaný systému v uceleném uzavřeném kódu.

3.3.3 Dropper

Dropper[27] funguje jako dopravní prostředek pro malware. Program nese ve svém nitru řadu jiných nežádoucích programů. Dropper si můžeme představit i jako instalátor jiného, avšak škodlivého softwaru. Dropper může přinést do systému mnoho malwarových programů, které pak škodí podle toho, jak byly naprogramovány (Hák, 2005).

3.3.4 Backdoor

Backdoor[28] umožňuje přístup ke vzdálenému systému prakticky odkudkoliv. Pokud se jedná o malware backdoor, jde o nelegální vniknutí do cizího systému. V takovém případě má útočník po úspěšném infikování systému možnost ovládat např. počítač napadeného a napadený o tom nemusí vůbec vědět. Velice dobře je backdoor popsán a vysvětlen Igorem Hákem: *„…aplikace, sloužící pro vzdálenou správu PC a sama osobě nemusí být škodlivá. Záleží pouze na osobě, která tuto vzdálenou správu vykonává. Pokud půjde o činnost škodlivou, pak tuto osobu nazýváme vzdáleným útočníkem. Princip fungování backdooru je následující. Klientská část vysílá požadavky útočníka serverové části, ta tyto požadavky plní, popřípadě odesílá zpět klientu požadované informace. Z předchozího je zřejmé, že klientskou část aplikace by měl vlastnit útočník a serverová by měla být umístěna na počítači, kde lze očekávat kupříkladu důležitá data. Pokud je serverová část backdooru vypouštěna úspěšně se šířícím virem, má vzdálený útočník k dispozici tisíce počítačů, ke kterým může vzdáleně přistupovat. Celá komunikace probíhá ve většině případů na bází TCP/IP, která ve spojení s celosvětovou sítí Internet umožňuje, aby útočník byl vzdálen tisíce kilometrů od serverové části backdooru.“* (Hák, 2005, s. 11).

3.4 Další druhy malware

Některé další druhy malware se nedají zařadit pouze k jednomu typu malwaru, neboť se vyznačují charakteristikami více z nich. Mohou mít více funkcí a jejich činnost není přímo omezena jedním způsobem chování.

[27] Z angl. jazyka: drop = položit, vypustit.
[28] Z angl. jazyka: backdoor = zadní vrata.

3.4.1 Logická bomba

Logickou bombou nazýváme cokoliv, co ve svém kódu obsahuje informaci o spuštění akce nepřímo uživatelem, ale událostí, která nastane při splnění určitých podmínek. Příkladem logické bomby může být spuštění destruktivní akce k datu pátku 13. Pokud byl infikován systém a zároveň je splněno kritérium, že je pátek 13., spustí se škodlivá činnost programu. Logickou bombou nemusí být pouze spuštění akce při datech, ke kterým se vztahuje pověrčivost. Program může být velice sofistikovaný a může fungovat tak, že při 1. spuštění vykoná zdánlivou slíbenou funkci doopravdy, ale při 2. spuštění může fungovat jako dropper a vpustí do systému jiný škodlivý software. Dále může být naprogramovaný tak, že pokud je program spuštěn zároveň s přehrávačem medií, může pak program mazat data z disku – příkladů může být nespočet, záleží pouze na tom, jak je naprogramován (Techtarget, 2005).

3.4.2 Phishing

Phishing[29] je velice zákeřná taktika, jejíž cílem je z nevinné oběti (většinou laika, který toho o podvodných praktikách moc neví) vylákat citlivé informace (např. odcizení PIN kódu od bankovního účtu). Phishing se vzdáleně může podobat trojskému koni, který má za úkol krást uživatelské údaje (password stealing trojan nebo keylogger), avšak nemusí se přímo nacházet v systému, ani nemusí systém přímo infikovat. V tomto případě se např. pouze stačí tvářit jako důvěryhodná stránka banky, kterou uživatel normálně navštěvuje. Ve skutečnosti se ale jedná o stránku, která má pouze vizuální vzhled té oficiální, její adresa je však odlišná. Stačí pak, aby uživatel zadal své přihlašovací údaje, které pak putují přímo k autorovi podvodně vypadajících stránek a autor škodlivého může nakládat se získanými informacemi podle svého (HOAX.cz, 2016).

3.4.3 Rootkit

Společnost AVG uvádí, že: *„Rootkit je aplikace (nebo skupina aplikací), která v počítači skrývá svoji přítomnost nebo přítomnost jiných aplikací (viry, spyware atd.)*

[29] Phishing vznikl spojením 2 anglických slov. Z angl. jazyka: fishing = rybařit a slangový výraz: phreaking = krádež. Fishing + phreaking = Phishing je tedy „rybařením“, kdy rybář je podvodník a loví „ryby“, uživatele, kteří se „chytí na návnadu“, a jsou následně podvodníkem okradení.

s využitím nižších vrstev operačního systému (přesměrování funkce rozhraní API[30]*, použití nezdokumentovaných funkcí operačního systému atd.). Díky tomu jej běžný anti-malwarový software prakticky nedokáže nalézt.“* (AVG, 2016).

3.4.4 Exploit

Veškeré kódy a programy, které kdy byly vytvořeny, většinou obsahují i chyby. Pokud program chyby obsahuje, vyvíjí se následně nové verze, kde se programátoři tyto chyby snaží opravit. Program, který funguje správně, ale jeho činnost se dá ovlivnit „zvenčí“ nějakou chybou má tedy nějakou bezpečnostní díru, které mohou autoři škodlivého kódu využít ve svůj prospěch a vytvořit tzv. Exploit. Exploit je program určený pro zákeřnou činnost, využívající úplné absence bezpečnosti, slabého bezpečnostního prvku nebo chyby v kódu. Jeden ze členů malajsijských hackerů, kteří se nazývají „Noobster Hexorcrew“ sám řekl, že: *„Exploit je pro mě vyloženě lahůdkou. Blbost někoho jiného, kdo mě sám vpustí do systému. Ten člověk si v podstatě nezamkne dům a ještě nechal otevřené dveře. Takový programátor musí nést zodpovědnost za své činy a nesmí se divit, když mu ten dům následně vykradu.“* (H4xor[31], nedat.).

3.4.5 Spyware

Spywarem[32] můžeme nazývat jakýkoliv program, který uživatele monitoruje bez jeho vlastního vědomí. Jak bylo popsáno výše, může se jednat o password stealing trojan malware, který má za úkol krást odposlechnuté informace od infikovaného uživatele. Může se však také jednat o programy, které obecně monitorují veškerou činnost uživatele bez jeho vědomí. Příkladem může být skenování aktivity uživatele na webu, sledování uživatelského dění na jeho monitoru apod. Mylně může být spywarem nazýván např. program VNC, jenž je někdy detekován i antiviry. Program VNC zaznamenává v reálném čase veškeré dění na jiném počítači. Tento program se používá např. ve firmách, kde se sleduje činnost zaměstnanců v pracovní době. Pokud byli zaměstnanci informováni o této

---

[30] API – Rozhraní pro programování aplikací. API ovládá funkcemi jiný zdrojový kód a může ovlivňovat program a jeho chování podle svých vlastních definovaných funkcí. API pak může ovládat přímo uživatel, nebo samotný rootkit přesměrováním těchto funkcí.

[31] H4xor – jeden ze členů skupiny „Noobster Hexorcrew“. Neoficiální spolupracovník mnoha antivirových firem. Napadá jejich systémy, maže data a upozorňuje na jejich bezpečnostní díry. Tuto činnost nedělá pro peníze, avšak pro slávu a uznání ze strany programátorů a IT nadšenců. Z důvodu nelegální činnosti špatně dohledatelný, avšak nechává o sobě vědět v místech, kde vykonal svoji nekalou činnost.

[32] Spyware vznikl spojením 2 anglických slov: spy = špehovat + software, software určený ke špehování uživatele.

skutečnosti, nejedná se o nelegální činnost, pokud se však tento program nainstaluje do systému bez vědomí a souhlasu uživatele, jedná se pak o trestnou činnost (Symantec, 2010).

3.4.6 Adware

Adware[33] byl známý i z dřívějších dob, avšak s vývojem doby se teprve až teď stal velice agresivním a nepříjemným jevem. Adware je software s reklamním materiálem. Tato reklama nemusí být nijak nepříjemná, využívá se například pro bezplatné užívání aplikace, která je zaplacena právě firmou, jejíž reklama je prezentována a ne uživatelem aplikace. Horší případ pak nastává tehdy, kdy je adware agresivnější a způsobuje nepříjemné vyrušování uživatele např. ve formě vyskakovacích bannerů, pop-upů a nebo přímo funguje jako přesměrování na podezřelé www stránky, kde se mohou nacházet jiné hrozby a formy malware. Na rozdíl od spyware je adware ve většině případů legální, protože je jeho použití obvykle popsáno v licenčním ujednání při instalaci aplikace nebo v podmínkách užití webu, kde se nachází. Pokud uživatel nesouhlasí s instalací adwaru společně s aplikací či programem, instalátor ho pak dál nepustí a aplikace se nenainstaluje (v případě webu s nesouhlasem se zobrazujícím se adwarem uživatele tento web přesměruje jinam). Někdy se však kombinuje s adwarem i „legální“ spyware, kdy je taky tento typ chování aplikace, programu, či webu popsano v podmínkách. Spyware pak skenuje uživatele a z výsledků, které přeposílá na analýzu může vzniknout cílený marketing „ušitý“ přímo na míru uživatele. Pokud však chybí ujednání a souhlas uživatele, jde pak o malware, protože je tato činnost prováděna bez vědomí uživatele, který toto jednání neschválil (PCTools, 2010).

Obrázek 5: Ukázka agresivního Adwaru ve formě automaticky vyskakujících POP-UP oken při brouzdání po internetu.

[33] Adware je odvozený od 2 anglických slov – z angl. jazyka: advertisement = reklama a software, dohromady spojeno v adware.

3.4.7 Ransomware

Jeden z posledních žhavějších trendů poslední doby. Když tvůrci malwaru zjistili, že formou malware se dá na obětech vydělávat finanční obnos, vytvářeli nejdříve keyloggery, které byly využívány k vykrádání bankovních účtu. Keyloggery však nebyly tak efektivní a jejich použití bylo navíc velice riskantní. Proto tvůrci malwaru vynalezli ransomware[34]. Jedná se o škodlivý software, který může mít formu trojského koně, červa nebo viru, kdy po infekci systému, dojde k zašifrování uživatelských dat (rozsah zašifrování záleží na naprogramování tohoto typu malware). Uživatel pak nemůže data používat do doby, kdy dojde k dešifrování jeho dat. Po infekci je uživatel obeznámen se svojí situací – pokud smaže program, který je zodpovědný za šifrování, ztratí tak možnost dešifrování jeho souborů, jelikož tento program zároveň většinou funguje jako dešifrovací zařízení. Dále je uživateli nabídnuto, že soubory budou dešifrovány za poplatek, který je nutno zaplatit autorům tohoto kódu. Po zaplacení je pouze na autorech malwaru, zda pošlou dešifrovací klíč nebo ne. Ve většině případů se ale autoři tohoto kódu chovají „čestně“ a poškozenému uživateli soubory vrátí zpět formou odkódování. V některých případech může být uživateli jedno, zda o soubory přijde, a to například v případě zálohovaných dat. Pokud se jedná o velice cenná data, která si napadený nezálohoval a není možnost jejich opětovného získání jinou cestou než odkódováním, „rád“ za dešifraci zaplatí (Trendmicro, nedat.).

3.4.8 Hoax

Hoax není přímo malware jako takový, nekoná škodlivou akci v počítačích, ale v lidských „hlavách“. Hoax je obecně poplašná zpráva, která má přinutit masu lidí uvěřit falešným informacím, takové informace však často mohou vyvolat povyk, zmatek, chaos nebo strach. Igor Hák o Hoaxu píše: Slovem: *„Hoax označujeme poplašnou zprávu, která obvykle varuje před neexistujícím nebezpečným virem. Šíření je zcela závislé na uživatelích, kteří takovou zprávu e-mailem obdrží. Někteří se mohou pokusit varovat další kamarády či spolupracovníky a jednoduše jim poplašnou zprávu přeposlat (forwardovat). Tím vzniká proces šíření. Ve speciálních případech lze do kategorie „hoax“ zařadit i zprávy, které třeba ani původně neměly být poplašné a nesouvisí s viry. Typickým příkladem jsou zprávy, kde*

---

[34] Ransomware vznikl spojením 2 anglických slov, z angl. jazyka: ransom = výkupné + software vznikl ransomware.

rodiče prosí o vzácnou skupinu krve pro svého umírajícího syna, jenž leží v konkrétní nemocnici. Vzhledem k tomu, že ale není uveden žádný časový údaj (popř. ho někdo „cestou“ smazal), tato zpráva může kolovat po Internetu i několik let.“ (Hák, 2005, s. 15).

4 Slavný malware

4.1 Morris Worm

Morris Worm[35] byl jeden z prvních počítačových červů, který ke svému šíření využíval síť internetu. Roku 1988 byl vytvořen 23letým studentem Robertem Tappanem Morrisem. Červ nebyl původně naprogramován pro škodlivou činnost, autor chtěl pouze zjistit počet připojených počítačů do internetové sítě. Kvůli chybě, kterou červ obsahoval, se ale původní dobrý úmysl minul účinkem. Infikovaný počítač mohl být červem infikován několikrát, protože červ neověřoval, zda se již někdy dříve v systému nacházel, proto k infikování těch samých počítačů docházelo stále znovu až na hranici jejich nepoužitelnosti. Počet infikovaných počítačů se odhadovalo na 6000 a byla způsobena škoda asi 100 milionů amerických dolarů (Techtarget, 2014).

4.2 ILOVEYOU

Červ známý pod jménem ILOVEYOU byl poprvé zaznamenán 4. května roku 2000 na Filipínách. Byl vytvořen v jazyce VBS[36], a proto bylo možné tímto červem infikovat pouze systémy Microsoft Windows. Po infikování se ILOVEYOU rozeslal na všechny adresy, které byly v infikovaném systému uloženy v adresáři aplikace Microsoft Outlook. Po odesílání svých kopií také ILOVEYOU přikládal přílohu, která už pro další škodlivou činnost potřebovala asistenci samotného uživatele. Po spuštění přílohy se hledaly v počítači čísla a hesla kreditních karet a mazaly soubory s příponami *.JPEG, *.MP3, *.VPOS, *.JS, *.JSE, *.CSS, *.WSH, *.SCT a *.HTA. Pro tehdejšího méně zkušenějšího uživatele byla znatelná hlavně ztráta obrázků a zvukových souborů. Odhad infikovaných počítačů čítá asi 45 milionů za jediný den (Techtarget, 2006).

4.3 Zeus

Jde o typ trojského koně, který napadá systémy od společnosti Microsoft Windows. Není primárně zaměřený jedním směrem, může vykonávat různé škodlivé funkce. Často je však využívaný ke krádežím bankovních informací metodou keyloggeru, ale také k instalaci samotného CryptoLockeru, nebo jako dropper jiného malwaru.

[35] Z angl. jazyka Morris Worm = Morrisův červ.
[36] Skriptovací jazyk založený na jazyce Visual Basic od firmy Microsoft.

Zeus se prvně objevil v červenci roku 2007 a je znám hlavně tím, že dokázal vytvořit jednu z největších zavirovaných sítí světa – tzv. botnet. Miliony počítačů pak vytváří jeho další kopie k rozesílání škodlivých informací. Navíc jsou tyto počítače a systémy společně propojeny a při správném naprogramování škodlivého softwaru se pak dá docílit vzájemné spolupráce.

Zeus je velice zrádný, a i v dnešní době je těžké ho detekovat kvůli jeho sofistikované architektuře a stealth prvkům (Kaspersky LAB, 2015).

4.4 Cryptolocker

CryptoLocker je malware typu ransomware/trojský kůň. Jeho první výskyt se datuje na rok 2013. CryptoLocker využívá důvěřivosti uživatele a po samotném otevření spustitelného souboru, který CryptoLocker obsahuje, se spustí šifrování souborů. Cryptolocker využívá velice silného šifrování[37], kdy kódování probíhá asynchronní metodou – je vytvořen jeden klíč na serveru a druhý pro samotného uživatele. Během následujících 72 hodin je uživatel nucen zaplatit „výkupné“ pro dešifraci svých souborů. Po uplynutí této doby se ze serveru klíč smaže. Uživatel, který nemá zálohu svých souborů, a nezaplatil do zmíněných 72 hodin určitou částku, se už pak k dešifrovacím klíčům nedostane, k dešifraci je totiž potřeba obou klíčů (Panda Security, 20015).

Obrázek 6: Oznámení Cryptolockeru o jeho výskytu v systému a instrukce k zaplacení poplatků pro poskytnutí klíče sloužícího k dešifrování uživatelských souborů.

[37] CryptoLocker využívá 2048-bitového šifrování. Pro běžné zabezpečené šifrování se používá 128-bitové až 256-bitové.

5 Prevence před malwarem

Nejlepší ochranou proti malware je samotná prevence. Ochranou před malwarem se přímo nemyslí antivirový program. Ten je jistě důležitým bezpečnostním prvkem v systému, avšak některé typy malware si snadno poradí, jak antivirus obejít. Firmy zabývající se vývojem antivirových programů ve většině případů pracují tak, že se snaží hledat choulostivá místa, odkud by šel systém infikovat. Tato „místa“ se snaží pojistit tak, aby k napadení nemohlo dojít. Mnohdy se ale stává, že je nalezen nebezpečný malware, a teprve poté se analyzuje a testuje jeho chování. Až na závěr se najde řešení, jak zamezit malwaru se do systému dostat.

Prvky, které můžeme zařadit do prevence je třeba firewall, zálohování systému a dat[38], obezřetnost na internetu a opatrnost při ukládání a otevírání neznámých emailů (včetně příloh podezřelých emailů). Je dobré se také vyvarovat „klikání“ na falešné/podezřelé reklamy a POP-UPy[39] odkazující na potencionálně nebezpečné stránky. Pokud se uživatel nenachází v domácím prostředí, měl by si dát pozor na sdílení souborů a přístupu do vlastního zařízení[40]. Není-li uživatel příliš zkušený, neměl by pracovat v prostředí, které má úplná práva správce[41] a v každém případě by měl být nainstalovaný aspoň nějaký antivirový program a mít ho řádně aktualizovaný. Pokud uživatel postupuje tímto způsobem, tak i v případě infekce a zhroucení systému může svoje data obnovit z vytvořené zálohy (viz výše).

5.1 Zálohování dat

Zálohování neboli úschova dat úzce s problematikou malware souvisí. Zálohou se zde myslí hlavně data na disku (popř. celý obraz systému, pokud je uživatel zkušenější), o která může potencionálně přijít v případě napadení škodlivým softwarem a následným formátování, smazáním dat nebo zašifrováním ransomwarem. Nejlepší je být připraven, a pokud dojde k poškození nebo infekci systému, nejjednodušší může být kompletní

[38] Zálohu je dobré uložit i mimo vlastní zařízení a to pro případ, že by potencionální škodlivý software mohl poškodit paměť, kde je záloha uložena. Flash disk, DVD nebo externí hard disk je proto velice moudrým řešením.

[39] POP-UP – vyskakující okno s reklamou, většinou odkazuje na potencionálně nebezpečné stránky.

[40] Souvisí to i přístupem na veřejné sítě wi-fi, kdy je možné kýmkoliv „odposlechnout“ příkazy odesílané do sítě a taky možnost „přijetí“ pozměněných přijímaných dat.

[41] Pokud je uživatel nezkušený a pracuje v admin režimu, může toho škodlivý software využít a zapisovat do oblastí, které jsou normálně nepřístupné.

formát systému a jeho opětovná instalace. Záloha pak zajistí, že uživatel neztratí žádná podstatná data.

Důležitý faktor, na který je třeba brát ohled, je interval, ve kterém by se zálohy měly provádět. Pokud uživatel zálohuje jedenkrát za rok, tak je velké riziko, že o data přijde mezi jednotlivými zálohami. Pokud ale uživatel bude zálohovat každý den, může ho to stát hodně zbytečného času a soustavným zápisem může snížit životnost svého paměťového media. Kompletní zálohu je tedy nejlepší provést jednou za čas (aspoň jedenkrát za 3 měsíce), ale soubory, které jsou pro uživatele cenné a důležité třeba zálohovat co nejčastěji a nejlépe na více míst (flash disk, cloud[42], externí disk apod.).

5.2 Firewall

Kasperksy LAB o firewallu[43] píše: *„Brána firewall slouží jako ochrana počítače proti virům, červům, trojským koním a hackerským útokům hrubou silou. Tato brána může být softwarová (bezpečnostní program) nebo hardwarová (fyzický směrovač), přičemž oba typy vykonávají stejnou funkci: prohledávají příchozí provoz, zda neobsahuje data nacházející se na seznamu zakázaných položek. Brány firewall prohledávají všechny pakety s daty (menší části větších celků, které jsou rozděleny kvůli snadnějšímu přenosu), zda neobsahují škodlivý kód. Tato činnost má různé podoby. Brány firewall v prvé řadě zachycují všechny požadavky na přístup a analyzují služby, které tyto požadavky vznášejí, s cílem ujistit se, že mají známý název domény a internetovou adresu. Tyto brány mohou rovněž kompletně prozkoumávat všechny pakety příchozích dat a vyhledávat v nich řetězce kódů nacházející se na seznamu zakázaných položek. V neposlední řadě pak brány firewall mohou vyhodnocovat pakety na základě jejich podobnosti s nedávno odeslanými a přijatými pakety. Splňují-li tyto pakety přijatelnou úroveň shodnosti, je jim přístup povolen.“* (Kaspersky LAB, 2015).

5.3 Antivirový program

Antivirový program byl poprvé vynalezen se záměrem identifikovat a zničit počítačové viry. Avšak s narůstajícími čísly reprezentující hrozby a útoky škodlivého kódu

[42] Z angl. jazyka Cloud = oblak. Cloudové úložiště je vzdálené úložiště dat, přístupné přes internet.
[43] Z angl. jazyka Firewall = ohnivá zeď. Firewall je jeden z bezpečnostních prvků pro eliminování rizika napadení malwarem.

provádějí developeři[44] nové výzkumy a vyvíjí pokročilé metody jak zabezpečit počítače proti škodlivému kódu. Antivirové programy byly vynalezeny pro skenování a identifikaci škodlivých hrozeb jako jsou viry a jejich okamžitou eliminaci. Většina z antivirových programů obsahuje automatické upozornění na nové aktualizace virové databáze (Comodo, 2016).

5.4 Administrátor VS uživatel

Pokud byly splněny všechny předešlé body, je třeba dát si pozor také na samotného uživatele. Pokud není uživatel zcela přesvědčen o svém počínání na počítači nebo není moc znalý, není na škodu, aby takový uživatel působil v systému s omezeným přístupem a přístupovými právy.

Některé systémy mají od výroby nastaveno, že první uživatel, který se přihlásí a vytvoří svůj učet, je také automaticky administrátorem. Být administrátorem a mít úplná práva znamená to, že dotyčný uživatel může nejen čist, ale i měnit a mazat data třeba v systémové oblasti, kde je jindy ostatním uživatelům přístup zamítnut. Pokud tedy méně znalý uživatel sám vymaže něco, co je v systému důležité, může způsobit pád systému i bez škodlivého softwaru.

Co se pak týče malwaru, administrátor jakožto méně znalý nebo zcela neznalý může dát přístup škodlivému softwaru do systémové oblasti (viz boot viry).

[44] Developer – v informatice člověk, jenž vyvíjí programy, vytváří nové, opravuje staré - ve svém oboru velice dobře orientovaný a znalý.

Praktická část

6 Znalost škodlivého kódu u žáků základních škol

V praktické části budu popisovat provedení a výsledky výzkumu znalostí škodlivého kódu u žáků základních škol. Výzkumná část zahrnuje dále vyhodnocení administrovaného dotazníku a analýzu získaných dat. Výsledky jsou diskutovány a uvedeny do širšího kontextu dané problematiky. V závěru uvádím nejdůležitější výsledky výzkumu.

6.1 Úvod k praktické části

Informační a komunikační technologie se sice na základních školách učí již od 1. stupně, avšak technický pokrok je dnes tak rychlý, že dítě má již před nástupem na druhý stupeň velké zkušenosti např. s chytrými telefony, počítači, tablety apod. Ve většině případech však problematiku malware s dítětem nikdo neprobírá (ať již rodiče nebo kdokoliv, kdo dítěti nabídne jistý přístroj). Možnost infekce samotného přístroje, nebo celé domácí sítě by mohlo vést až k vykradení bankovního účtu. Může se to sice zdát jako vyhrocený scénář, ale prevence je zajisté lepší, než následné řešení takového problému. Schopnost ovládání chytrých přístrojů žáky ZŠ i dětmi mladšími je na vysoké úrovni, předpokládá se ale, že znalost škodlivého softwaru nikoliv.

6.2 Cíl výzkumu

Cílem výzkumu praktické části je ověření znalostí žáků základních škol o škodlivém softwaru. Výzkum bude proveden formou anonymního dotazníku (viz kap. 6.4). Žákům předložíme otázky, které mají za cíl zjistit, zda žáci mají povědomí o pojmu malware. Dále chceme zjistit, jestli vědí, že škodlivý kód má nějaké členění, zda umí malware a škodlivý kód správně definovat a jaké mají povědomí o ochraně proti škodlivému kódu. Dále se budeme věnovat tomu, zda je rozdíl mezi znalostmi malwaru u chlapců a dívek, zda má v této oblasti vliv předešlá zkušenost s malwarem a jestli umí častěji malware a pojmy s ním spjaté správně definovat jedinec, který se považuje za technicky zdatného.

6.3 Formulace hypotéz a výzkumných předpokladů

Na začátku výzkumného procesu byly formulovány hypotézy a výzkumné předpoklady. Na základě vyhodnocení výzkumného dotazníku potom můžeme hypotézy přijmout, nebo zamítnout a také určit, zda jsou výzkumné předpoklady platné nebo neplatné.

Hypotéza 1: Chlapci umí pojem malware správně vysvětlit častěji než dívky.

Hypotéza 2: Žáci, kteří již byli v minulosti malwarem napadeni, umí tento pojem správně vysvětlit častěji.

Hypotéza 3: Žáci, kteří uvedli, že se považují za technický typ, umí pojem malware správně vysvětlit častěji, než žáci, kteří se za technický typ nepovažují.

Výzkumný předpoklad 1: Minimálně 50 % žáků má nějakou znalost o problematice malware a minimálně s 5 pojmy, které jsou s touto problematikou spjaty, se alespoň 50 % žáků již někdy setkalo.

Výzkumný předpoklad 2: Minimálně 50 % z žáků, kteří se minimálně s 5 pojmy týkajících se problematiky malware již někdy setkalo, neumí 5 a více pojmů týkajících se problematiky malware definovat správně.

Výzkumný předpoklad 3: Maximálně 30 % dotázaných žáků se považuje za technický typ.

6.4 Použitá výzkumná metoda

Pro realizaci výzkumu byla použita metoda dotazníku (Chráska, 2006). Tento anonymní dotazník obsahoval 18 otázek (2 otevřené, 8 uzavřených a 8 polouzavřených). Jelikož respondenti byli žáci základních škol, musely být otázky formulovány jednoznačně a jasně, aby je žáci pochopili, neztráceli se v nich a uměli na ně odpovědět bez pochyb. V případě, že by přece jen došlo k neporozumění, mohly být některé otázky žákům na místě lépe vysvětleny (záleželo na individuálním zhodnocení situace). Samotné pojmy nebo skutečnosti, které měly zhodnotit míru znalostí, vysvětlovány nebyly. Zkreslilo by to výsledky výzkumu nebo výzkum celý. Některé otázky byly polootevřené, aby žáci v případě chybějící možnosti v nabídce dotazníku mohli na danou otázku odpovědět vlastními slovy. Poslední otázka pak sloužila jako zpětná vazba (doplnění nevyřčeného nebo vzkázání námitky).

Otázky v dotazníku obsahovaly jak správné, tak špatné odpovědi. Tímto způsobem bylo možné žáky mírně zmást a ošetřit tak částečně to, zda pojmu doopravdy rozumí, či nikoliv. Některé matoucí odpovědi byly navázány na předešlé otázky, aby nebylo možné zpětně předešlé otázky správně zodpovědět na základě znalostí získaných z výčtu odpovědí v otázkách následujících. Jako příklad může být uvedena otázka č. 8, kde se v dotazníku táži, zdali žák ví, co je to pojem „firewall“. Jako matoucí odpověď je nabídnuta možnost, že „firewall“ je synonymum ke slovu „antivirový program“. V otázce č. 9 se zjišťuje, zda žák ví, co je to „antivirový program“ a jako matoucí možnost je nabídnuta odpověď, která odkazuje zpět na otázku č. 8, tedy že „antivirový program“ je pojem ekvivalentní pro pojem „firewall“.

Respondenti byli celkově v dotazníku tázáni na to, jaká zařízení používají, k čemu je používají, zda jim něco říkají pojmy: malware, počítačový virus, červ, trojský kůň, hoax, firewall, antivirový program. Dále také zjišťuji, zda se již žáci setkali s infekcí či napadením svého nebo jiného zařízení a jestli mají nějaké obavy z možné infekce vlastního zařízení. V dotazníku se objevila i otázka týkající se zálohování. Ke konci se dotazník zaměřuje na informovanost žáků ohledně problematiky malware, zda sám sebe považuje za technický typ a je mu nabídnuta možnost vzkázání námitky. Vlastní znění dotazníku je uvedeno v příloze 1.

6.5 Popis výzkumného vzorku a průběhu výzkumu

Výzkum probíhal u žáků na náhodně vybraných základních školách ve městě Olomouc. Dotazník vyplnilo 241 žáků, celkem 103 chlapců a 138 dívek. Šetření probíhalo na 3 základních školách, zkoumáno bylo celkem 12 tříd (vždy 3. třída, 4. třída 5. třída a 6 třída), průměrný počet dětí na jednu třídu bylo 20.

Nikdy nebyly zkoumány všechny třídy v jedné škole, a to buď z důvodu nedostupnosti žáků, časových důvodů, nebo to bylo přímo přání školy. V posledním případě si vedení nepřálo uskutečnit výzkum například z důvodu možného narušování některých z předmětů (skluz s učebním plánem apod.). Dva dotazníky musely být vyjmuty z šetření, protože byly vulgární a neměly žádnou výzkumnou hodnotu.

6.6 Použité metody pro analýzu a zpracování výsledků

Po sběru dat dotazníkovou metodou byla tato data analyzována a zpracovávána. Pro ověření hypotéz byl použit test nezávislosti chí-kvadrátu. Test nezávislosti se užívá v případech, kdy chceme zjistit, zda mezi jevy či skupinami existuje nějaká souvislost. Je třeba definovat nulovou a alternativní hypotézu. Nulová hypotéza předpokládá, že mezi jevy neexistuje souvislost. Alternativní hypotéza pak naopak souvislost či vztah mezi proměnnými předpokládá. K ověření hypotéz jsme stanovili hladinu významnosti α = 0,05 (hodnota, která počítá, s jak velkou pravděpodobností je možné určit správný výsledek) a je spočítána očekávaná četnost O (odpovídá případu platné nulové hypotézy). Hodnoty očekávané četnosti se vypočítají jako násobek odpovídající součtům pozorovaných četností u daných skupin, který je následně dělen četností celkovou.

Poté je pro každé pole kontingenční tabulky spočítána hodnota chí-kvadrátu, který je získán vztahem:

$$x^2 = \sum_{i=1}^{k} \frac{(Pi - Oi)^2}{Oi}$$

k zde označuje počet polí kontingenční tabulky, P je naměřená hodnota, O je hodnota očekávaná.

Je nutné určit stupeň volnosti, který je získán vztahem:

$$f = (r - 1) * (s - 1)$$

r zde je počet řádků, s pak počet sloupců jisté kontingenční tabulky.

Z tabulek je pak možné vyčíst hladinu významnosti, kritickou hodnotu a stupeň volnosti. Navzájem je pak srovnána kritická hodnota a hodnota získaná výpočtem. Nulovou hypotézu zamítáme v případě, že by vypočtená hodnota byla větší nebo rovna kritické hodnotě (Chráska, 2006).

6.7 Ověřování stanovených hypotéz

Ověřování jednotlivých, předem formulovaných hypotéz a jejich přijetí či zamítnutí.

6.7.1 Hypotéza 1

Hypotéza k ověřování: Chlapci umí pojem malware správně vysvětlit častěji než dívky.

Při ověřování hypotézy je nutné určit hypotézu nulovou, hypotézu alternativní a určit hladinu významnosti α, která je v našem případě α = 0,05.

Nulová hypotéza: Správné vysvětlení pojmu malware není závislé na pohlaví.

Alternativní hypotéza: Chlapci umí pojem malware správně vysvětlit častěji, než dívky.

Žáci byli rozdělení podle pohlaví a podle toho, zda definovali pojem malware správně nebo nesprávně.

Kontingenční tabulka - znalost pojmu malware - pozorované četnosti			
Pohlaví	Správná definice	Nepsrávná definice	Kontrolní součty
Chlapci	72	29	101
Dívky	88	50	138
Celkem	160	79	239

Tabulka 1: Pozorované četnosti definice pojmu malware v závislosti na pohlaví.

Kontingenční tabulka - znalost pojmu malware - očekávané četnosti Pearsonův chí-kvadrát: 1,487, sv = 1, p = 0,222224			
Pohlaví	Správná definice	Nepsrávná definice	Kontrolní součty
Chlapci	67,62	33,38	101
Dívky	92,38	45,62	138
Celkem	160	79	239

Tabulka 2: Očekávané četnosti definice pojmu malware v závislosti na pohlaví.

Ze statistického souboru vyšel chí-kvadrát: 1,487 při stupni volnosti = 1 s pravděpodobností chyby p = 0,222224 což přesahuje hladinu významnosti α = 0,05, v tomto případě přijímáme nulovou hypotézu: **Správné vysvětlení pojmu malware není závislé na pohlaví**, odmítnout nulovou hypotézu tedy nemůžeme.

6.7.2 Hypotéza 2

Hypotéza k ověřování: Žáci, kteří již byli v minulosti malwarem napadeni, umí tento pojem správně vysvětlit častěji.

Při ověřování hypotézy je nutné určit hypotézu nulovou, hypotézu alternativní a určit hladinu významnosti α, která je v našem případě α = 0,05.

Nulová hypotéza: Setkání s malwarem nemá se správnou definicí malwaru žádnou souvislost.

Alternativní hypotéza: Žáci, kteří již byli v minulosti malwarem napadeni, umí tento pojem častěji správně vysvětlit.

Žáci byli rozděleni na 2 skupiny podle toho, jestli definovali malware správně nebo ne v závislosti na tom, jestli již někdy malwarem napadení byli, či nikoliv.

Kontingenční tabulka - znalost pojmu malware - pozorované četnosti			
Napadení malwarem	Správná definice	Nepsrávná definice	Kontrolní součty
Někdy napaden	24	2	26
Nikdy nenapaden	136	77	213
Celkem	160	79	239

Tabulka 3: Pozorované četnosti definice pojmu malware v závislosti na předchozí zkušenosti.

Kontingenční tabulka - znalost pojmu malware - očekávané četnosti Pearsonův chí-kvadrát: 8,4803, sv = 1, p = 0,00359			
Napadení malwarem	Správná definice	Nepsrávná definice	Kontrolní součty
Někdy napaden	17,41	8,59	26
Nikdy nenapaden	142,59	70,41	213
Celkem	160	79	239

Tabulka 4: Očekávané četnosti definice pojmu malware v závislosti na předchozí zkušenosti.

Ze statistického souboru vyšel chí-kvadrát: 8,4803 při stupni volnosti = 1 s pravděpodobností chyby p = 0,00359. Jelikož tato hodnota hladinu významnosti α = 0,05 nepřesahuje, nulovou hypotézu odmítáme a potvrzujeme hypotézu alternativní: **Žáci, kteří jíž byli v minulosti malwarem napadeni, umí tento pojem častěji správně vysvětlit.**

6.7.3 Hypotéza 3

Hypotéza k ověřování: Žáci, kteří uvedli, že se považují za technický typ, umí pojem malware správně vysvětlit častěji, než žáci, kteří se za technický typ nepovažují.

Při ověřování hypotézy je nutné určit hypotézu nulovou, hypotézu alternativní a určit hladinu významnosti α, která je v našem případě α = 0,05.

Nulová hypotéza: Považování sebe sama za technický typ nemá žádnou souvislost s tím, jestli je malware definován správně.

Alternativní hypotéza: Žáci, kteří uvedli, že se považují za technický typ, umí vysvětlit malware častěji správně, než žáci, kteří se za technický typ nepovažují.

Kontingenční tabulka - znalost pojmu malware - pozorované četnosti			
Technický typ	Správná definice	Nepsrávná definice	Kontrolní součty
Ano	117	13	130
Ne	43	66	109
Celkem	160	79	239

Tabulka 5: Pozorované četnosti definice pojmu malware v závislosti na tom, zda se jedinec považuje za technický typ.

Žáci byli rozděleni na 2 skupiny podle toho, jestli definovali malware správně nebo ne v závislosti na tom, zda sami sebe označili za technicky zdatné, či nikoliv.

Kontingenční tabulka - znalost pojmu malware - očekávané četnosti Pearsonův chí-kvadrát: 68,462, sv = 1, p < 0,0001			
Technický typ	Správná definice	Nepsrávná definice	Kontrolní součty
Ano	87,03	42,97	130
Ne	72,97	36,03	109
Celkem	160	79	239

Tabulka 6: Pozorované četnosti definice pojmu malware v závislosti na tom, zda se jedinec považuje za technický typ.

Ze statistického souboru vyšel chí-kvadrát: 68,462 při stupni volnosti = 1 s pravděpodobností chyby $p < 0{,}0001$. Tato hodnota se ani vzdáleně nepřibližuje hladině významnosti $\alpha = 0{,}05$, nulovou hypotézu odmítáme a potvrzujeme hypotézu alternativní: **Žáci, kteří uvedli, že se považují za technický typ, umí vysvětlit malware častěji správně, než žáci, kteří se za technický typ nepovažují.**

6.8 Ověřování výzkumných předpokladů.

Ověřování jednotlivých, předem stanovených výzkumných předpokladů.

6.8.1 Ověřování výzkumného předpokladu 1

Výzkumný předpoklad 1: Minimálně 50 % žáků má nějakou znalost o problematice malware a minimálně s 5 pojmy, které jsou s touto problematikou spjaty, se alespoň 50 % žáků již někdy setkalo.

Výzkumný předpoklad zjišťoval kolik dotyčných žáků o problematice malware a pojmech s ním spojených aspoň někdy slyšelo.

Respondentů celkem	Mají povědomí o 5 a více pojmech	Mají povědomí o < 5 pojmech
239	132	107
100 %	55,23 %	44,77 %

Tabulka 7: Získané hodnoty znázorňující povědomí žáků o problematice malware a pojmy s ním spjaté.

Z tabulky č. 1 vyplývá, že celkový počet žáků, kteří májí znalosti o problematice malware a o pojmech už někdy slyšeli je větší než 50 %. Tímto se potvrdil výzkumný předpoklad č. 1, který tvrdí, že pojem malware je znám aspoň polovinou z celkově všech dotázaných žáků.

6.8.2 Ověřování výzkumného předpokladu 2

Výzkumný předpoklad 2: Minimálně 50 % z žáků, kteří se minimálně s 5 pojmy týkajících se problematiky malware již někdy setkalo, neumí 5 a více pojmů týkajících se problematiky malware definovat správně.

Tento výzkumný předpoklad říkal, že 50 % z žáků, kteří mají znalosti o malwaru, nebudou umět správně definovat 5 a více pojmů, které s touto problematikou souvisí.

Respondentů celkem	Správně definují 5 a více pojmů	Minimálně 5 pojmů nedefinují správně
132	71	61
100 %	53,79 %	46,21 %

Tabulka 8: Získané hodnoty znázorňující správné a špatné definování pojmů týkající se problematiky malware.

Z tabulky č. 2 lze vypozorovat, že výzkumný předpoklad 2 neplatí, protože více než 50 % žáků, kteří již o problematice malware slyšeli, umí 5 a více pojmů spojených s touto problematikou správně definovat.

6.8.3 Ověřování výzkumného předpokladu 3

Výzkumný předpoklad 3: Maximálně 30 % dotázaných žáků se považuje za technický typ.

Poslední výzkumný předpoklad očekává, že se mezi dotázanými žáky nebude nacházet více jak 30 % žáků, kteří se sami považují za technický typ.

Respondentů celkem	Označili se za technický typ	Neoznačili se za technický typ
239	103	136
100 %	43,10 %	56,90 %

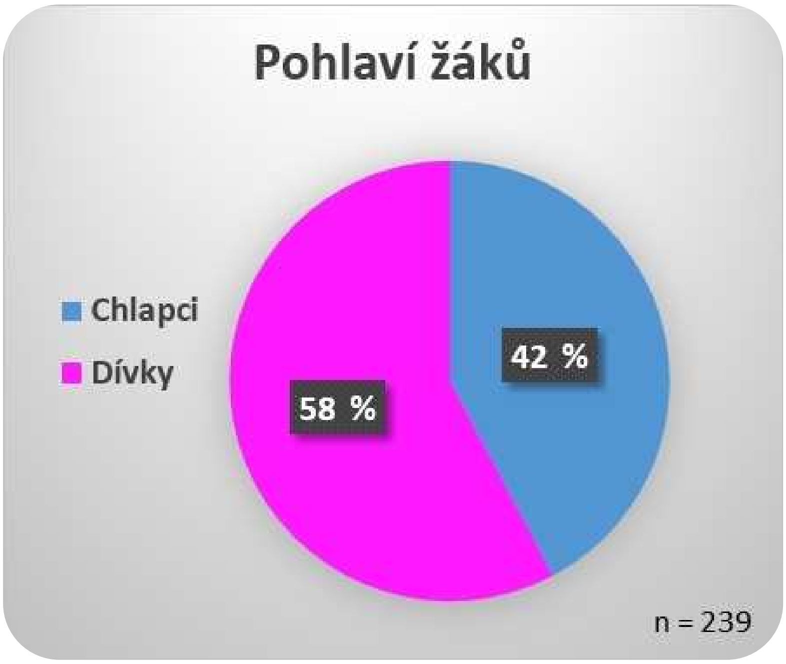
Tabulka 9: Získané hodnoty znázorňující žáky, kteří se buď za technický typ považují, či nikoliv.

Z tabulky č. 3 vyplývá, že výzkumný předpoklad 3 se nepotvrdil, protože předpokládal maximálně 30 % žáků, kteří sami sebe označí za technický typ.

6.9 Analýza vybraných odpovědí

6.9.1 Pohlaví respondentů

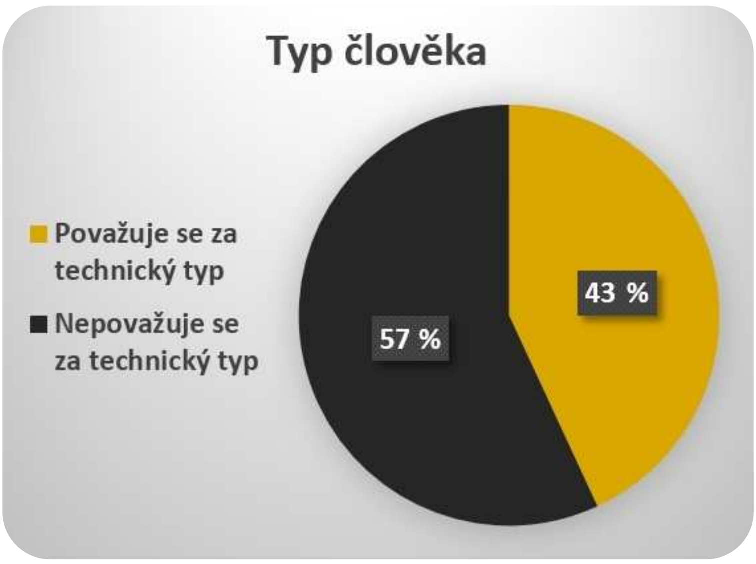
Dotazníkového šetření se účastnilo celkem 101 chlapců a 138 dívek. Jedná se o velice důležitou otázku, protože se váže k hypotéze č. 1.



Graf 3: Pohlaví žáků.

6.9.2 Technický VS netechnický typ

V otázce č. 17 jsem se žáků ptal na to, zda sami sebe považují za technický typ. Žáci, kteří sami sebe označovali jako technicky zdatné, uměli malware a pojmy s ním spjaté častěji správně definovat.



Graf 4: Za jaký typ člověka se považujete?

6.9.3 Využití přístroje - Stream

V otázce č. 2 jsem se dotazoval na využití přístroje. Někteří z respondentů napsali nad rámec nabízených odpovědí svoje vlastní, jiné využití - Streamování[45]. Tato odpověď v dotazníku chyběla, ale vzhledem k novým trendům, kdy se pomocí Streamu dají na internetu vydělat peníze, láká tato možnost i mladé lidi. Ti vidí své vzory ve starších, zkušenějších streamerech. Mladí streameři se pak pokouší tímto způsobem „prorazit do světa" s vidinou slávy nebo možností vydělat si peníze např. streamováním počítačových her.

Vzorek obsahoval 5 žáků, kteří streamují a všichni to byli chlapci.

6.9.4 Analýza malwaru a pojmů s ním spjaté.

V dotazníku se nacházelo 7 pojmů, které přímo s malwarem souvisely. Jednalo se o pojem malware, počítačový virus, červ, trojský kůň, hoax, firewall a antivirus. Odpovědi žáků na jednotlivé otázky jsou demonstrovány níže v grafu.

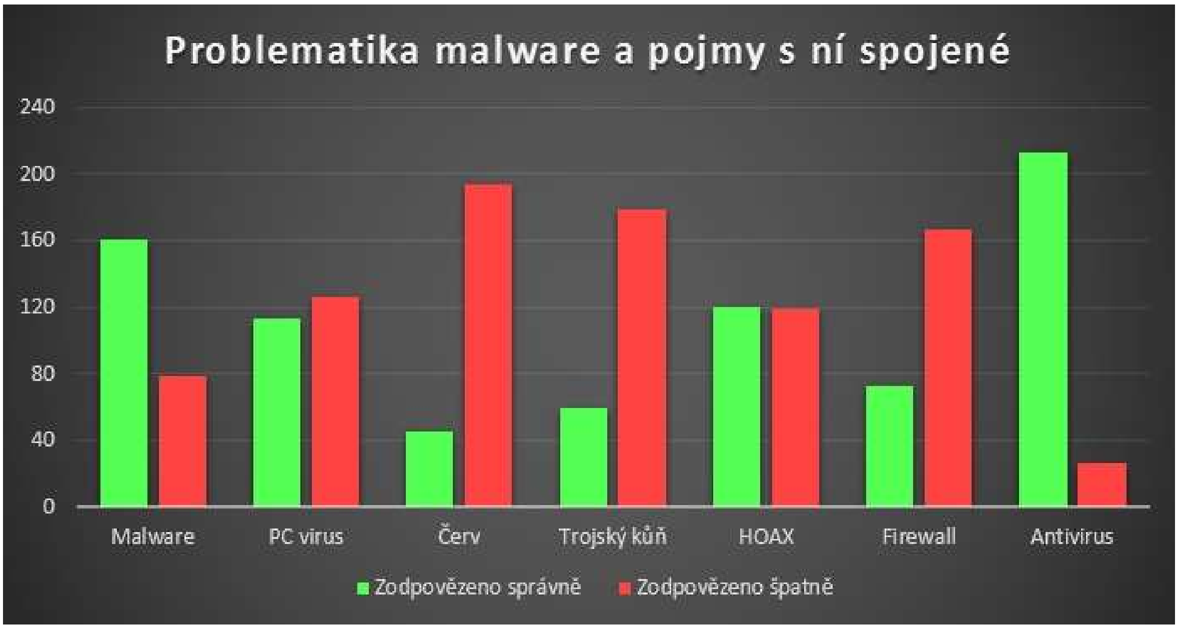
Pojem malware byl definován správně víc jak polovinou dotázaných žáků, horší to ale bylo s definicí počítačového viru, který žáci mylně označovali za synonymum malwaru.

V otázce č. 5 byli v dotazníku žáci tázáni na termín červ. Tuto otázku většina z dotazovaných zodpověděla špatně. Buď neodpověděli správně, nebo tento termín vůbec neznali.

Pojem trojský kůň dělal žákům taktéž velký problém. Žáci mnohokrát považovali trojského koně za pirátskou verzí jinak normálně placeného softwaru, nebo za software, který vyhledává cíleně malware jako takový. Domnívám se, že tato možnost mohla být žáky tipována, na základě znalosti mýtu o trojském koni. Vojáci z mytologického koně podle mě mohou děti mylně připodobnit k „antiviru", který zničil „malware" v Tróji. Tato myšlenka však nemusí být pravdivá, je to pouze autorova subjektivní myšlenka.

Pojem hoax uměli žáci vysvětlit „celkem" správně. Více jak polovina dotázaných žáků tento pojem definovala správně, velice úspěšně na tom také byl pojem antivirus, kdy nebyl nikdo, kdo by tento pojem neznal nebo nikdy neslyšel. Špatné odpovědi k pojmu antivirus se zde objevily proto, že si žáci tento pojem pletli s pojmem firewall.

[45] Stream – vysílání vlastního online kanálu (hráč např. hraje hru, kterou komentuje a nechává celý průběh „streamovat" online, aby ho mohli sledovat ostatní lidé, které vysílané téma zajímá), Streamer – člověk, který vysílá online.



6.9.5 Zajímavost – napadení učtu služby Steam

Někteří z respondentů (2 žáci ve vzorku) do obav z napadení napsali svoji vlastní obavu z napadení jejich Steam[46] účtu. Tito žáci se také označili za technické typy a o problematice malware měli dobré znalosti. Jejich odpovědi nebyly chybné a o škodlivém softwaru byli dobře informování.

jící odcizení

[46] Steam – platforma společnosti Valve Corporation. Společnost slouží k distribuci počítačových her online.

6.10 Diskuze

Z dotazníku bylo zjištěno, že žáci na základních školách disponují možnostmi využívání mnoha technických přístrojů. Všichni dotazovaní žáci mají doma k dispozici stolní počítač. Většina z nich také vlastní chytrý telefon, žádný z dotazovaných žáků neuvedl, že by neměl přístup k nějakému zařízení tohoto typu. Znalost škodlivého kódu však není zdaleka na tak dobré úrovni, jak by měla být, což také potvrdily výsledky výzkumu. Tato skutečnost je velice zarážející – drtivá většina žáků vlastní zařízení, se kterým umí pracovat, ale neuvědomují si rizika, která tato zařízení přinášejí nebo o rizicích vůbec nevědí. Můžeme usuzovat, že tato skutečnost je způsobena neadekvátním zařazením problematiky v RVP ZV[47] ve vzdělávací oblasti informační a komunikační technologie, nebo nedostatečným poučením o malwaru ze strany rodičů. Rodiče však nemusí svým dětem poradit z toho důvodu, že sami nemají o škodlivém kódu dostatečné znalosti. Srovnám-li výsledky s výzkumem Studené (Studená, 2015), ačkoliv byl prováděn na jiném vzorku, ukazuje se, že problematika neznalosti malwaru se netýká pouze dětí na základních školách.

Žáci, kteří o problematice malware už slyšeli, často špatně definovali pojmy a zaměňovali např. pojem malware a virus a naopak. Celkové znalosti škodlivého kódu těmito žáky proto nejsou na tak dobré úrovni, na jaké by měly být, v zásadě nedosahují ani základní úrovně. Tyto závěry se opět potvrdily i ve výše zmíněném výzkumu (Studená, 2015). Jak jsem již naznačil v kapitole o počítačových virech, za neznalost pravé podstaty tohoto a některých dalších pojmů může dle mého názoru chybné používání těchto pojmů médii. Žáci nejsou dostatečně poučeni ve škole a z médií získají nepřesné nebo dokonce chybné poznatky o malwaru.

Kromě žáků neznalých malwaru se ale objevili i žáci, kteří malware definovali správně a pojmy uměli dobře zařadit. Tito žáci se považovali za technické typy a technická zařízení využívali ve volném čase jako svůj koníček, nebo své záliby skrze tato zařízení provozovali, například streameři. Vzhledem k technickému pokroku, rychlému šíření informací přes sociální sítě a každodennímu využívání internetu nejen dětmi, ale i jejich rodiči, by se dalo předpokládat, že dětí, které budou znát malware a způsoby ochrany před ním bude v dnešní době mnohem více.

Celkově se tedy dá říct, že znalost škodlivého kódu žáky základních škol není celkově až tak špatná, ale stále je na nízké úrovni a tuto situaci by bylo dobré změnit.

[47] RVP ZV – Rámcový vzdělávací program pro základní vzdělání.

S dobrou znalostí škodlivého kódu se žáci budou moci lépe vypořádat s nepříjemnými situacemi, které mohou vzniknout, nebo budou aspoň vědět, jakým způsobem si počínat v případě napadení nebo infikování jejich zařízení malwarem. Situace může být zapříčiněna zastaralým nebo neadekvátním pojetím vzdělávací oblasti informační a komunikační technologie na základní škole, jak na úrovni RVP ZV, tak i ŠVP. Podkladem pro jejich aktualizaci ovšem musí být nějaké šetření, zjišťující aktuální stav znalostí malwaru u dětí, jako je například tato práce. Uvědomuji si, že vzhledem k rychle postupujícímu technickému pokroku je vidina RVP ZV sledujícího tento pokrok spíše utopická, ovšem jisté změny by zajisté měly být provedeny.

Závěr

Bakalářská práce „Problematika malware a znalost škodlivého kódu u žáků základních škol“ podala v teoretické části základní informace ohledně problematiky malware. Teoretická část byla věnována stručné historii malware a jeho vývoji. Byl nastíněn směr, kterým se nejspíše bude malware nadále ubírat. Definoval jsem škodlivý kód a dále ho rozdělil do skupin. Jednotlivé skupiny malwaru pak byly rozčleněny na dílčí celky a jednotlivě vysvětleny. Ke konci teoretické části jsem zmínil i malware, který se jistým způsobem proslavil a vzbudil mezi lidmi všeobecný zájem.

V praktické části se popisuji výzkum, který se zabýval znalostí škodlivého kódu u žáků základních škol. Výzkum byl proveden pomocí anonymního dotazníku, který byl podán k vyplnění 241 žákům. Stanovili jsme 3 hypotézy a 3 výzkumné předpoklady, které jsme chtěli ověřit. Data z dotazníků byla zpracována a analyzována metodou nezávislého testu chí-kvadrátu. Při námi stanovené hladině významnosti jsme přijali 2 alternativní hypotézy. Z výsledků vyplývá, že žáci základních škol mají určité povědomí o problematice malware, ale nejsou v ní příliš dobře orientovaní. Znalosti malware nemá souvislost s pohlavím žáků, existuje ale jistý vztah mezi znalostí a tím, zda se žák považuje za technický typ. Jako faktor zvyšující znalost problematiky malware u žáků je zkušenost s napadením jejich zařízení v minulosti, toto byla druhá přijatá hypotéza. Potvrdil se výzkumný předpoklad, že alespoň 50 % žáků bude mít o pojmu malware jisté povědomí. Další dva výzkumné předpoklady se ale neprokázaly jako pravdivé.

V diskuzi uvádím zjištěné výsledky do širšího kontextu a srovnávám je s výsledky výzkumu Studené. Dále se snažím vysvětlit možné příčiny aktuálního stavu a nakonec uvádím možnosti pro další výzkum.

Seznam zdrojů a bibliografických citací

40th anniversary of the computer virus. *HELPNETSECURITY* [online]. Moscow: HELPNETSECURITY, 2011 [cit. 2016-03-19]. Dostupné z: https://www.helpnetsecurity.com/2011/03/14/40th-anniversary-of-the-computer-virus/

Beating the Superbug: Recent Developments in Worms and Viruses. *SANS* [online]. Amsterdam: SANS Institute, 2002 [cit. 2016-03-21]. Dostupné z: https://www.sans.org/reading-room/whitepapers/malicious/beating-superbug-developments-worms-viruses-146

Cascade. *F-Secure* [online]. Helsinki: F-Secure, nedat. [cit. 2016-03-19]. Dostupné z: https://www.f-secure.com/v-descs/cascade.shtml

Co je brána firewall?. *Kaspersky LAB* [online]. Moscow: Kaspersky LAB, 2015 [cit. 2016-04-02]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/firewall

Co je stealth virus? *Kaspersky LAB* [online]. Moscow: Kaspersky LAB, 2015 [cit. 2016-03-19]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/stealth-virus

Co je to malware a jak se proti němu bránit. *Kaspersky LAB* [online]. Moscow: Kaspersky LAB, 2015 [cit. 2016-03-19]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/internet-safety/what-is-malware-and-how-to-protect-against-it

Co je to phishing. *HOAX.cz* [online]. Česká republika: HOAX.cz, 2016 [cit. 2016-04-02]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

Co je to rootkit?. *AVG* [online]. Amsterdam: AVG, 2016 [cit. 2016-03-20]. Dostupné z: https://support.avg.com/SupportArticleView?l=cs&urlname=What-is-rootkit

COHEN, Frederick. *Computer Viruses - Theory and Experiments: Computers & Security*. s. 23, North-Holland: Elsevier Science Publishers B.V., 1987, **6**. ISSN 0167-4048.

CryptoLocker: What is and How to Avoid it. *Panda Security* [online]. Spain: Panda Security, 2015 [cit. 2016-04-02]. Dostupné z: http://www.pandasecurity.com/mediacenter/malware/cryptolocker/

Facebook: Investor Relations. *Facebook Reports Third Quarter 2015 Results* [online]. USA: Facebook, Inc., 2015 [cit. 2016-03-19]. Dostupné z: http://investor.fb.com/releasedetail.cfm?ReleaseID=940609

HÁK, Igor. 2005. *Moderní počítačové viry* [online]. Hradec Králové, [cit. 2016-03-20]. Dostupné z: http://www.viry.cz/go.php?id=kniha/index. Bakalářská práce. Univerzita Hradec Králové. Vedoucí práce Doc. RNDr. Josef Zelenka, CSc.

CHRÁSKA, M. 2006. *Úvod do výzkumu v pedagogice.* Olomouc: VUP.
ISBN 80-244-1367-1.

ILOVEYOU virus. *Techtarget: Global Network of Information Technology, Websites and Contributors* [online]. Techtarget, 2006 [cit. 2016-04-02]. Dostupné z: http://searchsecurity.techtarget.com/definition/ILOVEYOU-virus

JAGODA, Ben. A short history of "Hack". In: *The New Yorker* [online]. USA New York: The New Yorker, 2015 [cit. 2016-03-20]. Dostupné z: http://www.newyorker.com/tech/elements/a-short-history-of-hack

Logic bomb (slag code). *Techtarget: Global Network of Information Technology, Websites and Contributors* [online]. Techtarget, 2005 [cit. 2016-04-02]. Dostupné z: http://searchsecurity.techtarget.com/definition/logic-bomb

Malware 101: Viruses. *SANS* [online]. Amsterdam: SANS Institute, 2016 [cit. 2016-03-21]. Dostupné z: https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

Malware History. In: *BitDefender* [online]. Bucharest: BitDefender, 2010 [cit. 2016-03-20]. Dostupné z: http://download.bitdefender.com/resources/files/Main/file/Malware_History.pdf

Malware: Definition. *Trendmicro* [online]. Irving, Texas: Trendmicro [cit. 2016-04-02]. Dostupné z: http://www.trendmicro.com/vinfo/us/security/definition/malware

Market share held by the leading computer operating systems worldwide from January 2012 to December 2015. *Statista: the statistics portal* [online]. Hamburg: statista, 2015 [cit. 2016-03-20]. Dostupné z: http://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/

Ministerstvo vnitra České republiky. Odbor bezpečnostní politiky. *Základní definice vztahující se k tématu kybernetické bezpečnosti* [online]. Praha, 2009. [cit. 2016-03-19] Dostupné z: www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

Ransomware: Definition. *Trendmicro* [online]. Irving, Texas: Trendmicro [cit. 2016-04-02]. Dostupné z: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware#logo

Robert Morris worm. *Techtarget: Global Network of Information Technology, Websites and Contributors* [online]. Techtarget, 2014 [cit. 2016-04-02]. Dostupné z: http://searchsecurity.techtarget.com/definition/Robert-Morris-worm

Smartphone OS Market Share, 2015 Q2. *ICD: Analyze the Future* [online]. Framingham: ICD, 2015 [cit. 2016-03-21]. Dostupné z: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

STAMP, Mark. *Information security: principles and practice*. 2nd ed. Hoboken, NJ: Wiley, 2011. ISBN 978-047-0626-399.

STUDENÁ, Michaela. 2005. *Problematika chápání pojmu malware u vysokoškolských studentů.* Olomouc, 2015. Bakalářská práce. Univerzita Palackého v Olomouci. Vedoucí práce: doc. PhDr. Miroslav Chráska, Ph.D

SZOR, Peter. *Počítačové viry – analýza útoku a obrana*. Překlad Ing. Lukáš Pelikán, Ing. Roman Skřivánek. 1. vyd. Brno : Zoner Press, 2006. 608 s. (Encyklopedie Zoner Press) ISBN 80-86815-04-8.

What are polymorphic viruses? *Techtarget: Global Network of Information Technology, Websites and Contributors* [online]. Techtarget, 2007 [cit. 2016-04-02]. Dostupné z: http://searchsecurity.techtarget.com/answer/What-are-polymorphic-viruses

What is a Boot Sector Virus?. *Kaspersky LAB* [online]. Moscow: Kaspersky LAB, 2015 [cit. 2016-03-19]. Dostupné z: https://usa.kaspersky.com/internet-security-center/definitions/boot-sector-virus#.VwUf8XqD5f4

What is Adware and Spyware? *PCTools* [online]. USA: Symantec, 2010 [cit. 2016-04-02]. Dostupné z: http://www.pctools.com/security-news/what-is-adware-and-spyware/

What is Antivirus Software? *Comodo: Creating Trust Online* [online]. New Jersey, USA: Comodo [cit. 2016-04-02]. Dostupné z: https://antivirus.comodo.com/what-is-antivirus-software.php

What is Elk cloner?. *Techtarget: Global Network of Information Technology, Websites and Contributors* [online]. Techtarget, 2014 [cit. 2016-04-02]. Dostupné z: http://searchsecurity.techtarget.com/definition/Elk-Cloner

What is Spyware and what does it do? *PCTools* [online]. USA: Symantec, 2010 [cit. 2016-04-02]. Dostupné z: http://www.pctools.com/security-news/what-is-spyware/

What Is the Difference: Viruses, Worms, Trojans, and Bots? *Cisco* [online]. [cit. 2016-03-19]. Dostupné z: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Zeus Trojan Malware. *Kaspersky LAB* [online]. Moscow: Kaspersky LAB, 2015 [cit. 2016-04-02]. Dostupné z: https://usa.kaspersky.com/internet-security-center/threats/zeus-trojan-malware-threat#

Seznam tabulek

Seznam obrázků

Seznam grafů

Seznam příloh

Příloha 1: Dotazník pro žáky základních škol.

Dotazník pro žáky

Dobrý den,

Jsem studentem UP v Olomouci, prosím o vyplnění tohoto anonymního dotazníku, který má za úkol zjistit, zda mají žáci ZŠ znalosti ohledně problematiky malware, popř. aspoň nějaké povědomí o škodlivém kódu. Výsledek bude použit pro moji bakalářskou práci: „Problematika malware a znalost škodlivého kódu žáky základních škol." Jak již bylo řečeno, dotazník je anonymní a výsledky nebudou poskytovány jiným osobám, prosím o pravdivé vyplnění (v případě neznalosti prosím netipujte správné odpovědi, nejedná se o test na známky a neznalost nebude penalizována).

Děkuji, Ladislav Orel.

1. **Jaké z následujících zařízení vlastníte? (Možné označit více odpovědí)**

   Chytrý telefon (telefon s otevřeným operačním systémem – tj. Symbian, Andoid, iOS, BlackBerry apod.)
   Stolní počítač
   Notebook
   Tablet
   Žádné z výše uvedených
   Jiné – uveďte prosím jaké:
   ……………………………………………………………………………
   ……………………………………………………………………………

2. **K jaké činnosti používáte technická zařízení? (Možné označit více odpovědí)**

   Hry, filmy, poslech hudby, media
   Návštěva sociálních sítí (FB, Twitter, MySpace, WK, Instagram apod.)
   Edukační účely a sebevzdělávání
   Vlastní tvorba (tvorba www, blog, apod.)
   Internetové bankovnictví
   Online nakupování (oblečení, PC hry, elektronika apod.)
   Stahování dat
   Zařízení nevlastním
   Jiná činnost:
   ……………………………………………………………………………
   ……………………………………………………………………………

3. **Říká Vám něco pojem „malware“?**

O tomto pojmu jsem v životě neslyšel

Pojem „malware“ označuje počítačový virus

Pojem „malware“ označuje občasnou nemoc počítačů. Malware může ohrozit fungování zařízení.

Pojem „malware“ označuje způsob, jak se bránit před škodlivým softwarem

Pojem „malware“ označuje celkově škodlivý software

Pojem jsem slyšel, ale nedokážu si pod ním nic představit

Moje představa je jiná (napište prosím Vaši představu):

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4. **Říká Vám něco pojem „počítačový virus“?**

„Počítačový virus“ je „malware“.

„Počítačový virus“ je škodlivý software, který může infikovat počítač.

„Počítačový virus“ je škodlivý software, který může infikovat počítač a může sám cestovat internetem.

Při infekci „počítačovým virem“ dochází ke zničení počítače.

O tomto pojmu jsem nikdy neslyšel.

Moje představa je jiná (napište prosím Vaši představu):

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

5. **Říká Vám něco pojem „červ“ v oblastí informačních technologií?**

Tento pojem jsem v životě neslyšel.

„Červ“ je výraz, který používají experti v oblasti IT pro pojem „počítačový virus“.

„Červ“ je škodlivý software, který může infikovat počítač a může sám cestovat internetem.

„Červ“ je díra v systému, která dovolí „počítačovému viru“ se do počítače dostat.

Pojem „červ“ jsem slyšel, ale žádná z předešlých odpovědí není správná, ale nevím, co si pod tímto pojmem představit.

Moje představa je jiná (napište prosím Vaší představu):

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

6. **Říká Vám něco pojem „trojský kůň“ v oblasti informačních technologií?**

Tento pojem jsem v životě neslyšel.

„Trojský kůň“ je škodlivý program, který však musí uživatel spustit sám, aby vykonal v počítači škodlivou činnost.

„Trojský kůň“ je program, který odhalí jiný škodlivý kód v počítači.

„Trojský kůň“ je nelegální verze placeného softwaru (např. Adobe Photoshop, či jiné placené programy „upravené“ tak, aby fungovaly i bez zaplacení).

Pojem „trojský kůň“ jsem slyšel, ale nevím co si pod ním představit.

Moje představa je jiná (napište prosím Vaší představu):

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

7. **Říká Vám něco pojem „HOAX“?**

„HOAX“ označuje nepravdivou informaci, která má za následek šíření zmatku, chaosu a nepravých informací.

„HOAX“ označuje varování před „počítačovými viry“.

„HOAX“ jsou servisní zprávy, které si technici počítačových sítí posílají pro vzájemné informování (něco jako rychlá SMS zpráva).

Pojem „HOAX“ jsem již někdy slyšel, ale nevím, co je to.

Pojem „HOAX“ jsem nikdy neslyšel.

8. **Říká Vám něco pojem „firewall“?**

Pojem „firewall“ označuje software pro detekci „počítačových virů“, poskytuje před nimi ochranu a dokáže je vymazat.

„Firewall“ funguje jako bezpečnostní prvek, který sleduje dění síťové komunikace a filtruje příchozí a odchozí data v počítači.

Pojem „firewall“ jsem v životě neslyšel.

Pojem „firewall“ jsem slyšel, ale nevím, co znamená.

9. **Říká Vám něco pojem „antivirus“?**

„Antivirus“ je jiný název pro „firewall“

„Antivirus“ označuje program, který dokáže detekovat škodlivý software, chrání počítač před infekcí a dokáže škodlivý software z počítače vymazat.

Pojem „Antivirus“ jsem neslyšel.

Pojem „Antivirus“ jsem slyšel, ale nevím, co znamená.

10. **Setkal/a jste se někdy s infekcí Vašeho zařízení?**

Ano.

Ne.

Nevím.

11. Z čeho byste měl/a strach, kdyby došlo k infekci Vašeho zařízení? (Vyberte max. 3 možnosti)

Ztráta dat.
Nevědomost toho, že jsem napaden popř. sledován.
Zpomalení mého zařízení.
Možnost nakažení ostatních zařízení, se kterými by moje zařízení přišlo do styku.
Únik mých citlivých dat, popř. jejich odcizení.
Ztráta přístupu k zařízení, nemožnost ovládat zařízení.
Nemám obavy.
Nemám žádné takové zařízení.
Měl bych jiné obavy. (Napište prosím jaké):
…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

12. Napište, co Vám říká pojem záloha v oblasti informačních technologií + jak často zálohujete (pokud tento pojem neznáte, nebo neumíte vysvětlit, pak tuto otázku přeskočte).

…………………………………………………………………………………
…………………………………………………………………………………
…………………………………………………………………………………

13. Máte ve škole povinné hodiny informační výchovy?

Ano (pokud ano, napište prosím, kolik máte vyučovacích hodin informatiky v týdnu)
…………………………………………………………………………………
Ne.

14. Informovala mě škola ohledně problematiky „malware“ a rizika, která jsou spjata s brouzdáním po internetu?

Ano
Ne
Nevím

15. Informoval Vás někdo jiný ohledně problematiky „malware“ a jiných rizik, které internet a brouzdání po něm přináší? (Možné označit více odpovědí).

Jsem informovaný ze školy
Informovali mě doma
Nikdo mě neinformoval, ale tyto informace se ke mně občas nějak dostanou samy (internet, televize, spolužáci apod.)

Jsem informovaný dobře sám/sama. Tyto informace vyhledávám sám/sama a vzdělávám se i v této oblasti.
Nikdo mě neinformoval

16. Jste:

Muž
Žena

17. Považujete sebe sama za technický typ? (Rozumím dobře počítačům, novým technologiím, velice rychle se umím naučit s novým zařízením, které jsem nikdy předtím neviděl apod.)

Ano
Ne

18. V případě, že něco v dotazníku chybělo a Vy to považujete za důležité, napište to prosím.

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………

ANOTACE

Jméno a příjmení:	Ladislav Orel
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	doc. PhDr. Miroslav Chráska, Ph.D.
Rok obhajoby:	2016

Název práce:	Problematika malware a znalost škodlivého kódu u žáků základních škol.
Název v angličtině:	The issues of malware and knowledge of malicious code by students at elementary schools.
Anotace práce:	Bakalářská práce pojednává o problematice malware se zaměřením na její znalost žáky základních škol ve výzkumné části. Dobrá orientace v oblasti malware a znalosti škodlivého kódu dnes není dostatečná, jedná se však o důležitou oblast, která by neměla být zanedbána. Teoretická část obsahuje úvod do problematiky malware, vývoj a rozčlenění škodlivého kódu, uvedeny jsou slavné škodlivé kódy a zabývám se též prevencí a ochranou před škodlivým kódem. V praktické části je popsán výzkum znalostí malwaru u žáků základních škol. Data byla sebrána metodou dotazníku na vzorku 241 žáků, následně vyhodnocena a analyzována pomocí testu nezávislosti chí kvadrát. Z výsledků vyplývá, že znalosti malwaru u žáků základních škol nejsou dostačující. Výsledky byly diskutovány a shrnuty v závěru práce.
Klíčová slova:	Malware, škodlivý kód, počítačový virus, červ, trojský kůň, prevence před malwarem, firewall, antivirový program, znalosti malware, základní škola, dotazník.
Anotace v angličtině:	This bachelor thesis is focused on research about malware knowledge by students at elementary schools. Nowadays people are not well informed about malware, but malicious code should not be taken lightly. Theoretical part of work consist prelude for malware problematics, evolution of malicious code, malware is

	sorted by its type, there were stated famous types of malare and the end of theoretical part is dedicated for prevention against malware. In practical part there is described research which is focused on elementary school students. Data were gathered and analysed by method of questionnaire. There were 241 students, who filled form in. Data from questionnaires were evaluated by method of chi square distribution. Results were discussed and conclusions were drawn.
Klíčová slova v angličtině:	Malware, malicious code, computer virus, worm, trojan horse, prevention against malware, firewall, antivirus, malware knowledge, elementary school, questionnaire.
Přílohy vázané v práci:	1
Rozsah práce:	51 stran + 5 stran příloh
Jazyk práce:	Český