Digitální učební materiál

Projekt	CZ.1.07/1.5.00/34.0415 Inovujeme, inovujeme						
Šablona	III/2 Inovace a zkvalitnění výuky prostřednictvím ICT (DUM)						
DUM č.	**32_Ch**65_1_13	ŠVP	**Fotograf**				
RVP	**34-56-L/01 Fotograf**		Ročník	**1.**	Předmět	**INF**	
Zpracoval(i)	**Mgr. Petra Jurtíková**					Kdy	**III/2013**
TC/Téma/klíčová slova	**Informatika/Malware/Kosmetička-vizážistka, Kosmetické služby, Fotograf, malware, viry, backdoor, spyware, trojský kůň, červ, hoax, antivirový program**						

Anotace

DUM obsahuje prezentaci na téma „Malware“, prezentaci s úkoly pro studenty a stejné úkoly zpracované do interaktivního dokumentu v programu MS Word. Úvodní prezentace slouží jako výklad pro studenty. Samotná prezentace obsahuje také úkoly k tématu, které studenti řeší během výkladu a zápisu, popřípadě je mohou dostat zadány za domácí úkol. Pro učitele jsou zde i řešení těchto úkolů. Úkoly jsou propojeny na vyhledávání informací pomocí internetu, popř. vyhledávání informací na počítači. Použije-li se zamknutí dokumentu s úkoly v MS Word, mohou studenti doplňovat pouze na daná místa text či obrázek.

Druh výukového zdroje: prezentace, pracovní listy v MS PowerPoint a pracovní listy v MS Word

Typ interakce: frontální, skupinová

Soubor název	Soubor – popis obsahu
32_Ch65_1_13 Malware.pptx	Prezentace učiva, teoretická část, úkoly a odpovědi
32_Ch65_1_13 Malware – úkoly1.pptx	Prezentace úkolů pro studenty s místem pro vložení odpovědí
32_Ch65_1_13 Malware – úkoly2.docx	Úkoly pro studenty s místem pro vložení odpovědí

Metodický list

Se studenty probereme dané téma pomocí úvodní prezentace, mezitím si studenti dělají zápis elektronicky v MS Word, nebo si zapisují do sešitu či používají interní studijní texty. Během teoretického výkladu jsou v prezentaci vloženy otázky nebo úkoly, které studenti vyhledávají na internetu, v samotném počítači nebo vytvářejí přímo sami. Tato zadání jsou interaktivně zpracována pomocí odkazů v prezentaci. Studenti mají k dispozici pro své odpovědi buď prezentaci, kde je místo na doplnění odpovědí, nebo dokument v MS Word, který po zamknutí slouží jako šablona pouze pro doplňování. Nakonec všechny odpovědi a nalezené výsledky zkonzultujeme

společně. Úkoly v MS Word jsou připraveny pro skupinové řešení, pro dvě skupiny. Prezentace s úkoly je tvořena formou frontální.

Další možnost plnění úkolů je, že prezentaci se zadanými úkoly dostanou studenti formou domácího úkolu, který po splnění odevzdají na Moodle.

Veškeré odpovědi k otázkám, jak z prezentace pro studenty, tak z úkolů v MS Word, má učitel dostupné v úvodní prezentaci. Zde je vždy otázka a hned odpověď či obrázek, popř. návod na splnění daného úkolu.

Malware a antiviry

úkoly

Zpracovala: Petra Jurtíková

Střední škola
potravinářská,
obchodu a služeb Brno
Charbulova 106

Úkol 1

- **Najděte na internetu**
  - z jakých anglických slov vzniklo slovo Malware
  - a co znamenají v překladu
- **Odpověď**

Úkol 2

- **Najděte na internetu**
  - jakýkoliv text hoaxu
- **Odpověď**

Úkol 3

- **Zjistěte doma i ve škole**
  - jaký máte antivirový program
  - celý jeho název
- **Odpověď**

Skupina A

1. Najděte na internetu:
   a) z jakých anglických slov vzniklo slovo Malware

      45T

   b) co znamenají v překladu

      45T

2. Najděte na internetu:
   a) nějaký text hoaxu

      45T

Skupina B

1. Najděte na internetu:
   a) jaký máte antivirový program

      45T

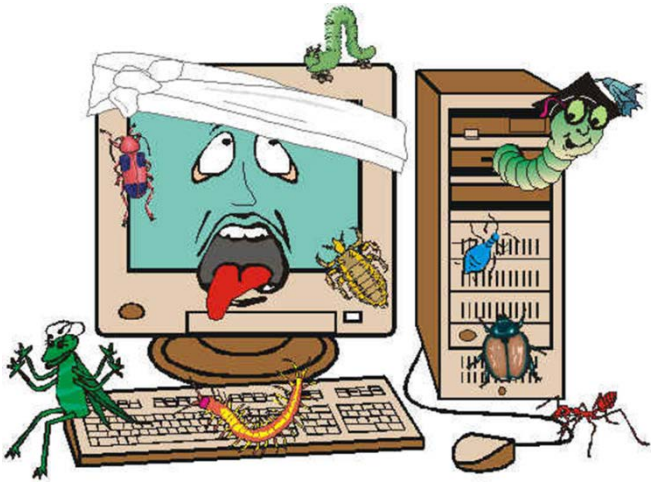
   b) napište celý jeho název

      45T

2. Najděte na internetu:
   a) nějaký text hoaxu

      45T

Malware a antiviry



aneb my se čertů nebojíme

Zpracovala: Petra Jurtíková

Střední škola
potravinářská,
obchodu a služeb Brno
Charbulova 106

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Prezentace a úkoly

- **Části prezentace:**
  - výklad
  - úkoly
- **Výklad**
  - zápis do textového editoru, sešitu či studijní materiály
- **Úkoly**
  - rozdělení do skupin
  - hledání zadaných úkolů
  - uložení do textového editoru (i obrázky)
  - popř. zadáno jako domácí úkol

Historie

- **Termín počítačový virus byl poprvé použit v roce 1972**
  - ve vědecko-fantastickém románu Davida Herolda When Harley Was One (neodpovídá dnešnímu pojetí)
- **Termín počítačový virus byl poprvé definován Fredem Cohenem v roce 1983**

- **První virus**
  - na počítačích třídy IBM PC s operačním systémem MS-DOS
  - objevil se v lednu 1986 – pákistánský virus Brain

Malware

Úkol 1

- **Malware**
  - je počítačový program určený ke vniknutí nebo poškození počítačového systému
  - vznikl složením anglických slov

  - zahrnují se sem všechny počítačové viry, trojské koně, spyware a adware
  - nesprávně se vše označuje **Viry**

Funkce virů

- název odvozen od biologických virů (podobné vlastnosti)
- vkládá sám sebe do jiných programů (infikuje je)
- provádí nějakou (většinou) škodlivou činnost
- snaží se utajit před uživatelem a antivirovým programem
- dokáže se sám šířit bez vědomí uživatele
- při spuštění hledá další vhodný soubor pro množení

Vlastnosti malware

- **Současné počítačové viry**
  - mohou smazat obsah paměti Flash-BIOS a tím znemožnit chod počítače
  - virus se nemusí vždy odstranit, neboť kód viru může být zapsán ještě v Master Boot Recordu (MBR)
- **Existují „mýty“ o poškozování FDD, HDD, monitorů**
  - většinou však jde o chybně navržená zařízení
  - může dojít ke zničení v rámci zahlcení RAM, disku …

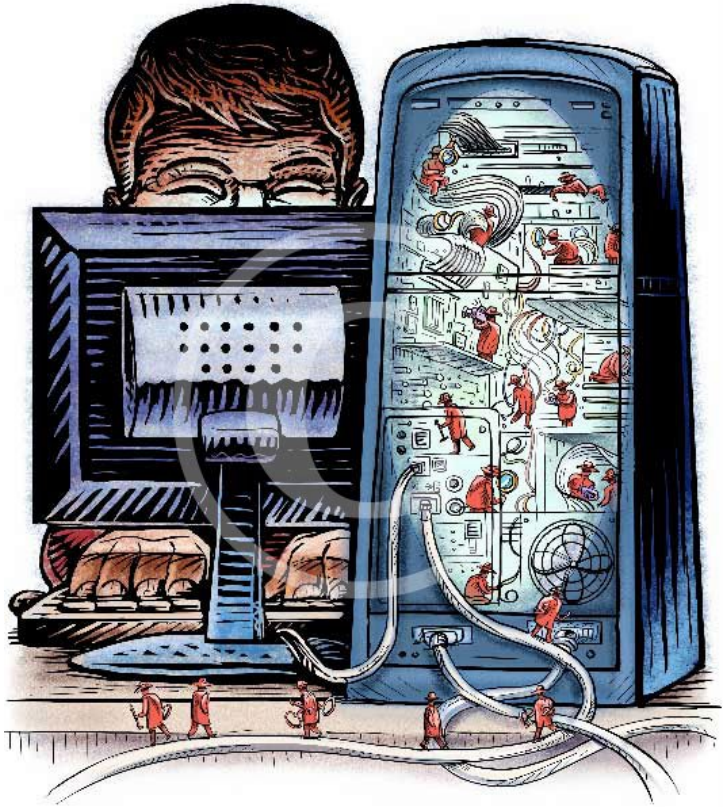
Způsob šíření virů

- **Paměťové médium**
- **Síť**
  - lokální
  - Internet
- **Moderní prostředky**
  - Bluethoot

- **V současné době napadají**
  - počítače
  - chytré telefony

Proč se šíří viry

- **Díky bezpečnostním chybám**
  - v systému
  - v programech
- **Díky uživatelům**
  - crack, vypínání firewallu
  - přeposílání spamu



Dělení virů

- **Boot viry (Boot Viruses)**
  - napadají boot sektor, MBR a tím si zajistí své spuštění hned při startu počítače
- **Souborové viry (File Viruses)**
  - jejich hostitelem jsou soubory
- **Multipartitní viry (Multipartite Viruses)**
  - napadají více částí (boot sektor i soubory)
- **Makroviry (Macroviruses)**
  - šíří se v prostředí aplikací podporujících makra (MS Word, MS Excel)

Projevy virů

- Destrukce dat
- Zobrazování různých zpráv na obrazovce
- Vyluzování různých zvuků a melodií (Yankee Doodle)
- Vtipkování s uživatelem (vkládání vtipných komentářů do textových souborů, různé animace, ...)
- Simulace selhání technického vybavení
- Zpomalování činnosti počítače

Tak nějak se začínalo

Jsem albánský počítačový virus
ABDUL.exe.
S ohledem na mizivé možnosti mé
země ti nemůžu nic udělat.
V rámci humanitární pomoci si smaž
ve svém počítači nějaký soubor
a předej mě dál!

Pojmenování virů

- **Autorem viru**
  - Brain, Alabama
- **Místem svého odhalení**
  - Durban, Suomi, Taiwan
- **Činností, kterou provádí**
  - Flip, Ping-Pong, Jo-Jo, Yankee Doodle
- **Délkou, o níž zvětšuje infikované soubory**
  - 405, 5120, 4096
- **Datem aktivace**
  - Friday 13th, December 24th, Advent

Vznik virů

- **Programátoři**
  - pomsta
  - zničit firemní síť nebo poškodit firmu
  - vyzkoušet své schopnosti, touha po slávě, legrace
- **Firmy vytvářející antivirové programy**
  - za účelem zvýšení prodeje svých výrobků
- **Ovládnutí a řízení většího množství počítačů**
  - využívat je např. k rozesílání spamu
- **Nebo jen snaha škodit, ničit, ublížit**

Základní dělení virů

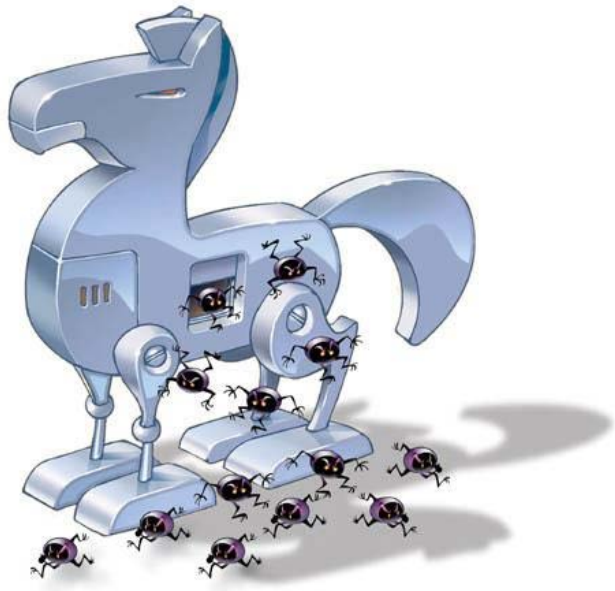
- **BACKDOOR**
  - IRC
- **TROJSKÉ KONĚ**
  - PASSWORD STEALING
  - DESTRUKTIVNÍ
  - DROPPER
  - DOWNLOADER
  - PROXY TROJAN
- **ČERVI (WORMS)**
  - SQLSlammer
  - LOVSAN / BLASTER
- **SPYWARE**
  - ADWARE
  - DIALER
  - HOAX
  - KEY LOGGER

Vlastnosti

- **BACKDOOR**
  - program otevírá v PC zadní vrátka a umožňuje neoprávněný vzdálený vstup do PC a zde provádět cokoliv (mazat, získávat data, vypínat)
  - používají hackeři
- **IRC**
  - komunikující v IRC síti (propojení více serverů)
  - jeví se jako skutečná chatující osoba
  - útočník se může do napadeného PC zalogovat a domluvenými rozkazy vzdáleně ovládat

Vlastnosti

- **TROJSKÉ KONĚ**
  - chová se jako legální program, ale provádí škody (antivirový program – maže soubory na HDD)
  - stačí odmazat tento soubor
  - není schopen množení

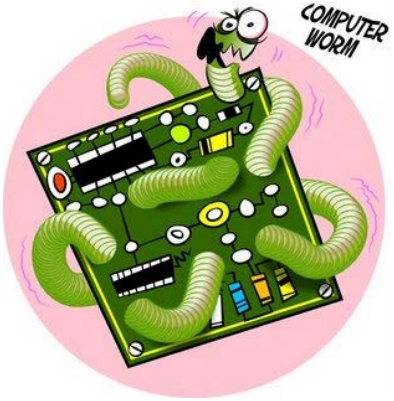


Vlastnosti

- **PASSWORD STEALING - TROJANI (PWS)**
  - sleduje jednotlivé stisky kláves, ukládá je a odesílá na dané e-mailové adresy majitelům virů
- **DESTRUKTIVNÍ TROJANI**
  - likviduje soubory na disku nebo ho rovnou zformátuje
- **DROPPER**
  - vypouštěč – nese v sobě jiný škodlivý vir
- **DOWNLOADER**
  - spustitelný soubor z Internetu uložen na disk, který zajistí spuštění dalších souborů z internetu
- **PROXY TROJAN**
  - zneužití PC pro odesílání SPAMU

Vlastnosti

- **ČERVI (WORMS)**
  - první označení pro tzv. Morrisova červa, který v roce 1989 dokázal zahltit síť
  - pracují na nižší síťové úrovni než ostatní viry
  - šíří se síťovými pakety v síti Internet od infikovaného systému
- **SQL SLAMMER**
  - v aplikaci MS SQL Server
  - pouze zahltí celou LAN síť produkcí paketů
- **LOVSAN/BLASTER**
  - pouze hlášení o chybách v OS



Spyware

- **Zákeřnost a nebezpečí**
  - je statická a nešíří se tak v počítači
- **Projevy**
  - šíří se společně s řadou sharewarových programů
  - stahování a instalaci dalšího škodlivého softwaru
  - vykrádání citlivých informací uživatele a odesílat je útočníkovi (certifikáty, hesla pro přístup k bankovnímu účtu, PINy, navštěvované stránky...)
  - odesílání nevyžádané pošty - SPAMu

Spyware

Úkol 2

- **ADWARE**
  - znepříjemňuje práci s PC reklamou, „vyskakující“ reklamní okna během surfování s vynucováním stránek
- **HOAX**
  - poplašná zpráva, která varuje před neexistujícím virem
  - šíření e-mailem ve snaze informovat další
- **DIALER**
  - přesměrování telefonní linky na drahé tel. tarify (60 kč/min)
- **KEY LOGGER**
  - sleduje pohyb na klávesnici, odesílá pak uživatelova hesla

Antivirové programy

- **Nejznámějšími antivirovými a antispywarovými programy jsou**
  - AVG, AVAST, Norton Security Scan, Norton Antivirus, Spyware Terminator, Spyware Doctor, MS Security Essentials …
- **Slouží k**
  - detekci a odstranění počítačových virů
  - prevenci proti případné nákaze
- **V dnešní době**
  - je známo desetitisíce různých počítačových virů

Zabezpečení dat

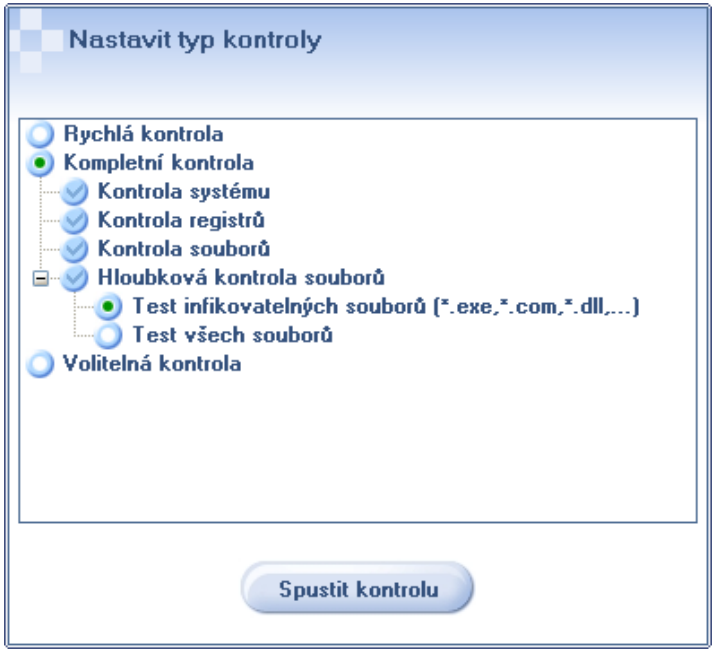
- **Zabezpečení ochrany před neoprávněným manipulováním se zařízeními**
  - zabránění přístupu nepovolaných osob k částem počítačového systému
- **Bezpečnostní prvky**
  - přidělení rozdílných práv zaměstnancům
  - autorizační systémy chráněné hesly

Prevence

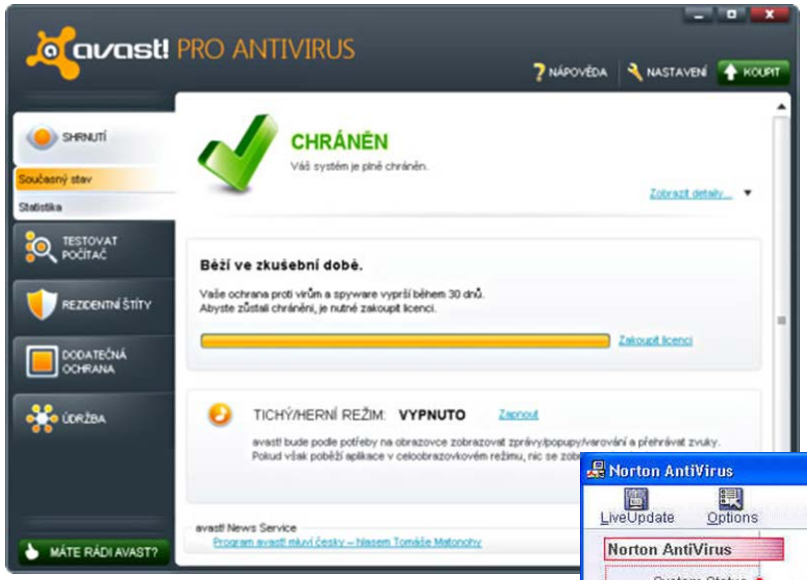
- **Programy**
  - používat legální programové vybavení
  - používat antivirové programy (popř. antispywarové, či antispamové programy)
  - provádět pravidelné aktualizace antivirových programů
- **Internet**
  - u neznámých dokumentů MS Office zakázat makra
  - neotvírat přílohu e-mailu od neznámého odesílatele
  - nespouštět žádné podezřelé programy (z Internetu)
- **Zálohovat důležitá data**

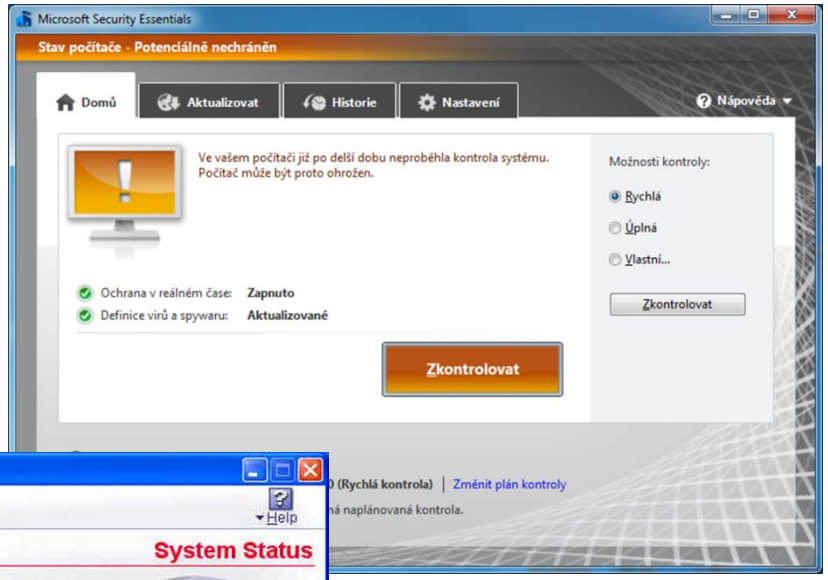
Antivirové programy

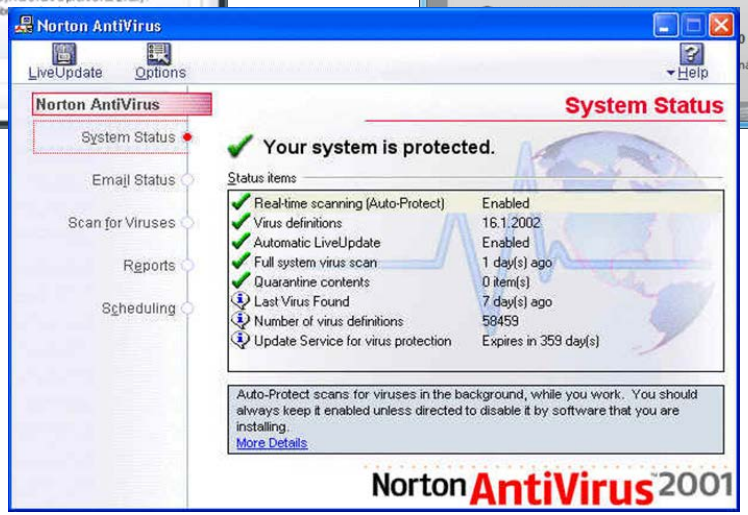
- **Aktualizace (Avast)**
- **Nastavení kontroly (Spyware Terminator)**



Antivirové programy







Antivirové programy

Úkol 3

Použité zdroje – teorie

- **Str. 1**
  - MOODLE TŘEBEŠÍN. *Programové vybavení*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.moodle-trebesin.cz/course/view.php?id=21>.
- **Str. 3**
  - LOGIC LOUNGE. *Malware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://logiclounge.com/2010/11/23/how-to-avoid-malware/>.
- **Str. 4**
  - GYMNÁZIUM. *Počítačový virus*. [online]. [cit. 2012-12-28]. Dostupné z: <www.gymkh.cz/student/Informatika/zadani/.../Počítačový%20virus.ppt>.
- **Str. 5**
  - PC VIRUSY. *Počítačový červ*. [online]. [cit. 2012-12-28]. Dostupné z: < http://www.pcvirusy.estranky.sk/clanky/cervy-worms.html >.
- **Str. 7**
  - ANTIVIROVÉ CENTRUM. *Viry*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.antivirovecentrum.cz/aktuality/podle-analytiku-esetu-je-mezi-hrozbami-na-prvnim-miste-celosvetove-stale-inf-autorun.aspx>.
- **Str. 8**
  - ONLY THE CONS. *Spyware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://onlythecons.com/mywebsearch-one-of-todays-most-frequent-spywaretrojans-information-removal/>.
- **Str. 9**
  - MFS. *Malware na USB*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.mfs-theothernews.com/2013/01/stuxnet-going-rogue-malware-infects-us.html/>.
- **Str. 10**
  - MEMEBURN. *Malware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://memeburn.com/2011/04/six-malware-milestones-from-brain-to-anna-kournikova/>.
- **Str. 11**
  - PALBA.CZ. *Nový počítačový virus*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.palba.cz/viewtopic.php?f=5&t=23&start=60>.

Použité zdroje – teorie

- **Str. 12**
  - STELLA PHOENIXS. *Malware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://stellarphoenixs.wordpress.com/>.
- **Str. 13**
  - CULT OF MAC. *Virus*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.cultofmac.com/188296/new-mac-malware-steals-all-the-passwords-you-enter-into-your-browser-logs-your-keystrokes/>.
- **Str. 15**
  - SECURITY STRONGHOLD. *Backdoor*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.securitystronghold.com/solutions/gumblar-removal-tool-download.html>.
- **Str. 16**
  - DREAMS TIME. *Trojský kůň*. [online]. [cit. 2012-12-28]. Dostupné z: < http://www.dreamstime.com/stock-images-threat-trojan-virus-image12507804 >.
- **Str. 18**
  - NEJELPŠÍ ANTIVIRY. *Počítačový červ*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.nejlepsi-antiviry.cz/pocitacovy-cerv-cervi-a-jejich-kamaradi//>.
- **Str. 19**
  - DATACENTER. *Sypyware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.shopdatacenter.com/virus-trojan-spyware-and-malware-removal/>.
- **Str. 21**
  - SERVIS PC. *Odvirování počítače*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.servispckupka.cz/odvirovani.php>.
- **Str. 23**
  - NETCLARITY. *Malware*. [online]. [cit. 2012-12-28]. Dostupné z: <http://www.netclarity.net/technology/malware-cleanup-utilities>.

Malware a antiviry

úkoly a odpovědi

Zpracovala: Petra Jurtíková

Střední škola
potravinářská,
obchodu a služeb Brno
Charbulova 106

Úkol 1

Zpět

- **Najděte na internetu**
  - z jakých anglických slov vzniklo slovo Malware
  - a co znamenají v překladu
- **Odpověď**
  - „malicious“ (zákeřný) a „software“ (program)

Úkol 2

Zpět

- **Najděte na internetu**
  - jakýkoliv text hoaxu
- **Odpověď**
  - www.hoax.cz

Verze 1 z října 2010

SKANDÁL:mlékárenské společnosti mohou ze zákona prošlé mléko až pětkrát přepasterizovat a uvést znovu do prodeje,
Je nutno velmi dobře prohlédnout tetrapack, jestliže najdete 12 45 - tj. chybí 3 - pak se jedná o mléko, jež třikrát prošlo a bylo třikrát přepasterizované. A ovšem v krabici je každé balení jiné. De facto pijeme špinavou vodu!

Verze 2 léto 2011

Tetrapaková mléka, co zde kupuji, to mají taky. Recyklují to po celé Evropě. Kamarád má známou na hygieně v Bělehradě a ta mu to prozradila. Za 14 dní to bylo i v tamních novinách: www.vesti-online.com/Vesti/Srbija/155705/Ima-li-u-Srbiji-recikliranog-mleka (*poz. redaktora: ZDE je strojový překlad*)

Takže dobrou chuť.
Pro ty, kteří textu neporozumí:
Mléko v tetrapaku, které se nespotřebuje do konce trvanlivosti, prodejce vrátí zpracovateli. Zpracovatel otevře obal, mléko opětovně převaří a opět zabalí. Mohou tak učinit max. 5 krát. Zespodu krabice je pod zalepeným záhybem číslo 12345, jedno z čísel chybí. Tato chybějící cifra udává, kolikrát už bylo mléko "recyklováno". tj. 12 45 znamená, že bylo převařeno 3 krát.
Tak dobrou chuť.

Úkol 3

Zpět

- **Zjistěte doma i ve škole**
  - jaký máte antivirový program
  - celý jeho název
- **Odpověď**
  - AVG
  - AVG Anti-Virus Business Edition 2012