Podpora spolupráce
škol a firem

# Projekt Pospolu

## MALWARE – bezpečný počítač

*Autorem materiálu a všech jeho částí, není-li uvedeno jinak, je Bohuslava Čežíková.*

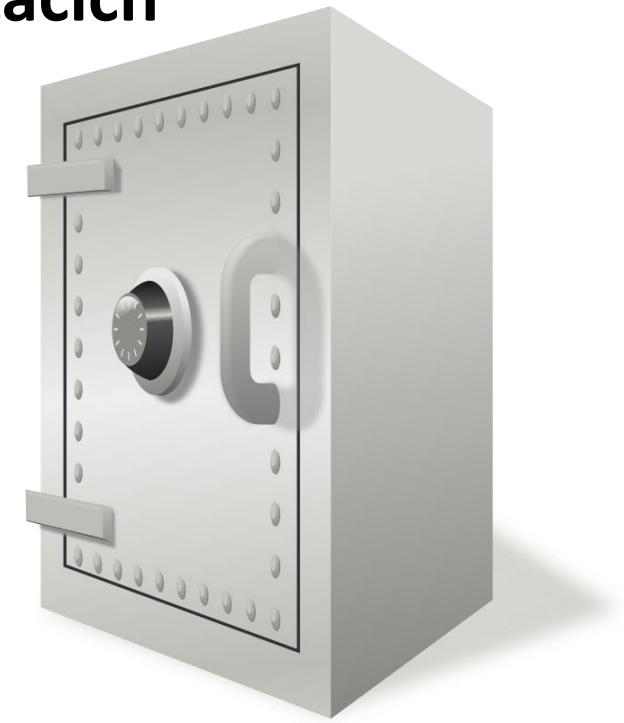
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

# Škodlivý software

- **počítačová rizika**
- **malware – jednotlivé typy**
- **malware podle umístění v paměti**
- **malware podle napadené oblasti**
- **malware podle projevů chování**
- **zabezpečení počítače**

# Počítačová bezpečnost

- **obor informatiky**
- **zabývá se zabezpečením dat v počítačích**



**Obr. 1: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<https://openclipart.org/detail/126241/safe-by-rg1024>.**

# Počítačová rizika

- **vnitřní rizika – mohou se projevit například kolizí programu, nechtěným smazání dat, zkratem apod.; způsobují je zejména softwarové chyby, hardwarové chyby a chyby uživatele**
- **vnější rizika – důsledek nedostatečného fyzického zabezpečení počítače nebo absentující softwarové ochrany, firewallu (krádež počítače, poškození vnějšími vlivy a počítačová infiltrace)**

# Malware

- **malicious + software = škodlivý software**
- **po spuštění škodí výpočetnímu systému**
- **může být spuštěn přímo z počítače, do kterého byl přenesen, nebo může počítač napadnout na dálku**

# VIR

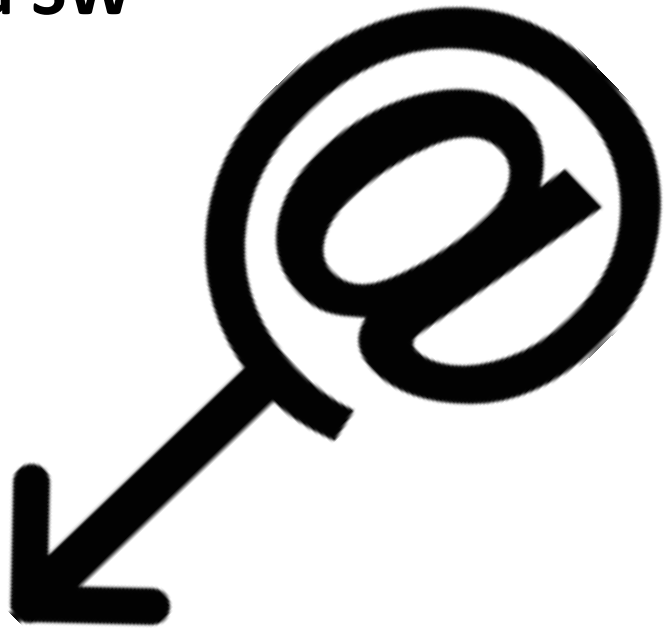
- **program, který parazituje na již existujícím souboru**
- **může se nekontrolovatelně replikovat nebo zahájí destrukční operace – tím dojde k poškození, změně nebo zničení dat, ke stahování dalšího malware apod.**

# Trojský kůň

- **neumí se replikovat**
- **jeho činnost se zahájí okamžitě nebo ho aktivuje konkrétní událost**
- **typ spyware – shromažďování informací**
- **typ adware – nevyžádaná reklama, nahrazování reklamních bannerů**

# Červ

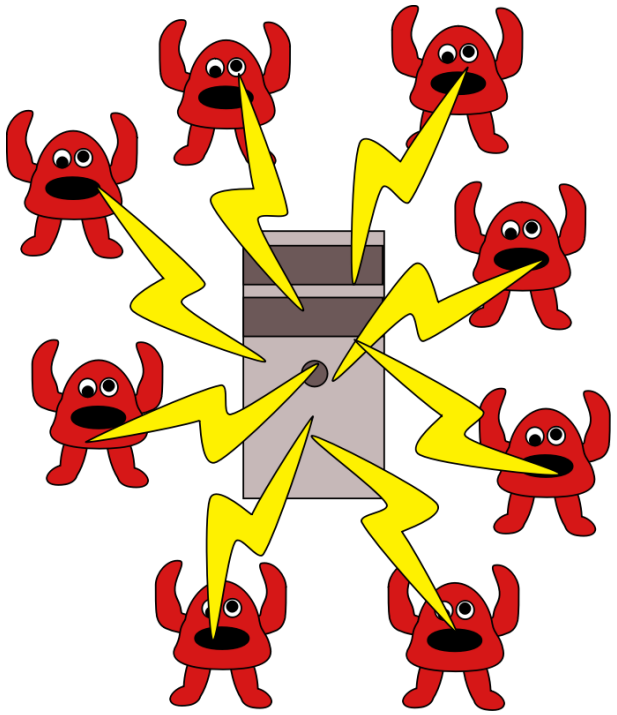
- **šíří se pomocí počítačových sítí (příloha e-mailu)**
- **využívá bezpečnostní díry v OS a SW**



**Obr. 2: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<**https://openclipart.org/detail/61783/an-attack-happened-here-by-andy_gardner**>.**

# Backdoor

- **Zadní vrátka – neautorizovaný vstup do PC**



**Obr. 3: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<**https://openclipart.org/detail/204734/denial-of-service-attack-by-clickschool-204734**>.**

# Logic bomb

- **Logická bomba – skrytý kód vložený do běžného programu**
- **může se šířit pomocí viru, červa nebo jiným způsobem**

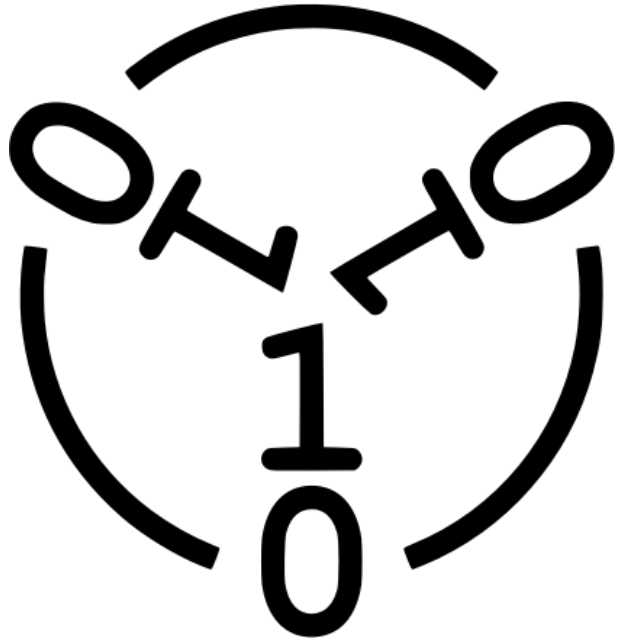
# flooder

- **zombie = počítač, nad kterým převzal kontrolu hacker**
- **pomocí zombie je generován velký síťový provoz**

# Exploit

- **přes slabé místo programu proniká do výpočetního systému**
- **využívá se pro testování možností průniků do systému**

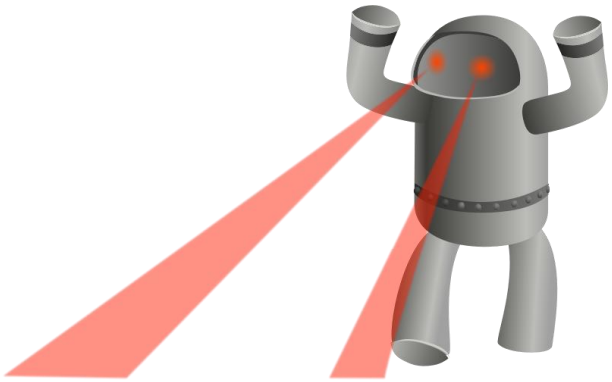
- **jeho cílem je instalovat do počítače virus – ten je obvykle zakódován (problém s odhalením)**




**Obr. 4: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<**https://openclipart.org/detail/898/proposed-malware-warning-symbol-by-ronkaminsky**>.**

# injektor

- **zvláštní druh drooperu**
- **instaluje kód viru do paměti počítače**



**Obr. 5: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<**https://openclipart.org/detail/208615/rampaging-robot-by-anarres-208615**>.**

# Malware podle umístění v paměti

- **rezident – umístěný v paměti; infikuje soubory, s nimiž provádí výpočetní operace**
- **nerezident – aktivuje se spuštěním hostitelského programu; po své činnosti vrací řízení hostitelskému programu**

# Malware podle napadené oblasti

- **souborový – napadá spustitelné programové soubory**
- **bootvir – napadá systémové oblasti HDD**

  **nebo tabulku MBR**

# Malware podle projevů chování

- **makrovir – pozměňuje sady příkazů využívané programy k provádění obvyklých činností (obvykle kancelářské aplikace)**
- **stealth vir – využívá maskování**
- **polymorfní vir – vytváří různé mutace**

# Zabezpečení počítače



- **antivirová ochrana**
- **Firewall**
- **software pro auditování**

**Obr. 6: [cit. 2013-10-02] Dostupný pod licencí Public domain na** WWW: **<**https://openclipart.org/detail/134161/security-icon-by-gsagri04**>.**

# Zdroje

[1] BROOKSHEAR, J. Glenn. *Informatika*. Brno: Computer Press, 2013. ISBN 978-80-251-3805-2.
[2] ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: Teoretická učebnice*. Brno: Computer Press, a. s., 2010. ISBN 978-80-251-3228-9.
[3] SZOR, Peter. *Počítačové viry - analýza útoku a obrana*. Brno: ZONER software s.r.o., 2006. ISBN 80-86815-04-8.
[4] Saferinternet.cz [online]. [cit. 2014-10-25]. Dostupné z WWW: <http://www.saferinternet.cz/>.
[5] BRAIN, Marshall a Wesley FENLON. *How stuff works:* „How Computer Viruses Work“. [online]. [cit. 2014-10-05]. Dostupné z WWW: <http://computer.howstuffworks.com/virus.htm>.
[6] Computer virus (virus). Webopedia [online]. [cit. 2014-11-05]. Dostupné z WWW: <http://www.webopedia.com/TERM/V/virus.html>.
[7] Viry.cz [online]. [cit. 2014-10-10]. Dostupné z WWW: <http://www.viry.cz/>.
[8] JUNEK, Pavel. Zálohování.net: *„Zálohování a archivace dat v podnikovém prostředí – 6. díl (část 1/3), Business Continuity Management (BCM)“*. [online]. [cit. 2014-10-17]. Dostupné z WWW: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-6-dil-cast-13-business-continuity-management-bcm/>.
[9] HÁK, Igor. Moderní počítačové viry: třetí vydání [online]. 2005 [cit. 2014-10-16]. Dostupné z WWW: <http://viry.cz/download/kniha.pdf>.
[10] Přispěvatelé Wikipedie, Počítačová bezpečnost [online], Wikipedie: Otevřená encyklopedie, c2014, Datum poslední revize 3. 07. 2014, 09:14 UTC, [citováno 07. 10. 2014] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost&oldid=11635583>.
[11] IT slovník [online]. [cit. 2014-10-10]. Dostupné z WWW: <http://it-slovnik.cz/>.
[12] Openclipart [online]. [cit. 2014-10-02]. Dostupné pod licencí Public domain z WWW: <https://openclipart.org/homepage>.