SLEZSKÁ UNIVERZITA
FILOZOFICKO-PŘÍRODOVĚDECKÁ FAKULTA V OPAVĚ

Šárka Vavrečková

Operační systémy I

Praktikum z operačních systémů

Bezpečnost a pořádek

Slezská univerzita v Opavě
Filozoficko-přírodovědecká fakulta
Ústav informatiky

Opava, poslední aktualizace 1. listopadu 2023

Anotace: Tento dokument je určen pro studenty druhého ročníku IVT na Ústavu informatiky Slezské univerzity v Opavě. První část semestru je věnována systému Windows, druhá část systému Linux; tento dokument obsahuje témata společná pro oba systémy. Zabýváme se zde především:

- bezpečností systémů obecně: role aktualizací systému a aplikací, škodlivý software (malware), obrana proti malwaru,
- právními aspekty používání (jakýchkoliv) systémů, především licencemi.

Praktikum z operačních systémů, Operační systémy I

Bezpečnost a pořádek

RNDr. Šárka Vavrečková, Ph.D.

Dostupné na: http://vavreckova.zam.slu.cz/pos.html

Ústav informatiky
Filozoficko-přírodovědecká fakulta v Opavě
Slezská univerzita v Opavě
Bezručovo nám. 13, Opava

Sázeno v systému LaTeX

Obsah

1 Díra nedíra... 1

1.1 Děravý systém . . . 1
1.2 Automatické aktualizace systému . . . 6
1.3 Aktualizace aplikací . . . 6
1.4 Hesla . . . 8
1.5 Sociální inženýrství . . . 10

2 Malware 12

2.1 Malware podle toho, jak se k nám dostane . . . 12
2.1.1 Virus . . . 12
2.1.2 Trojský kůň . . . 14
2.1.3 Červ . . . 16
2.2 Malware podle působení . . . 17
2.2.1 Spyware . . . 17
2.2.2 Rootkit . . . 18
2.2.3 Ransomware . . . 19
2.2.4 Další typy malwaru . . . 20
2.3 Co s tím? . . . 22
2.4 Spam . . . 24
2.5 Botnet . . . 24

3 Nástroje proti malwaru 27

3.1 Bezpečnostní produkty . . . 27
3.1.1 Antispam . . . 27
3.1.2 Antivirový software . . . 28
3.1.3 Antispyware . . . 29
3.2 Firewall . . . 30
3.3 Podle čeho vybírat bezpečnostní produkt . . . 32
3.4 Mobilní a další zařízení . . . 32

4 Projekty a licence 34

4.1 Základní pojmy . . . 34
4.2 Nejpoužívanější licence . . . 36
4.2.1 Licence určené pro software . . . 36

4.2.2 Licence určené pro dokumenty 38
4.2.3 Kombinování licencí 39

Kapitola 1

Díra nedíra. . .

Rychlý náhled: Tato kapitola je úvodem do zabezpečení počítače, přičemž většina zde uvedených informací se týká různých operačních systémů. Začneme bezpečnostními problémy operačních systémů a aplikací, rolí aktualizací, následují sekce o heslech a sociálním inženýrství.

Klíčová slova: Bezpečnostní mezera, zranitelnost, CVE, bezpečnostní scanner, aktualizace, buffer overflow, stack overflow, heslo, hash, správce hesel, sociální inženýrství

Cíle studia: Po prostudování této kapitoly se budete orientovat v pojmech používaných pro popis bezpečnostních zranitelností. Zjistíte důležitost včasných aktualizací jak operačního systému, tak i aplikací, naučíte s vytvořit si silné heslo a bezpečným způsobem ho používat.

1.1 Děravý systém

Mnozí uživatelé žijí v přesvědčení, že jejich počítač je vlastně zcela nezajímavý a proto není nutné se obávat napadení počítače. Ve skutečnosti je pro hackera (útočníka) z různých důvodů zajímavý prakticky každý počítač, do kterého se mu podaří dostat. Proč?

- hesla, přístupové certifikáty, atd., také například do banky,
- „citlivé dokumenty“ s osobními či firemními informacemi, jsou použitelné pro vydírání nebo třeba poškození firmy, dále třeba filmy a hudba, kontakty,
- zajímavé jsou také zdroje počítače – místo pro uložení „cizích“ dat, čas procesoru, apod.,
- když nic jiného, počítač může fungovat jako *zombie* (také *bot*, počítač vzdáleně ovládaný bez vědomí majitele, obvykle k nezákonným účelům) – sítě botů se používají například při rozesílání spamu nebo tzv. DDoS útokům (účelem je kolaps vybraného serveru),
- „smyslem“ útoků může být také obyčejná zákeřná snaha zničit co se dá,
- zařízení může sloužit jako rukojmí – prostřednictvím vyděračského softwaru (ransomwaru).

Malware je souhrnný název pro škodlivý software.

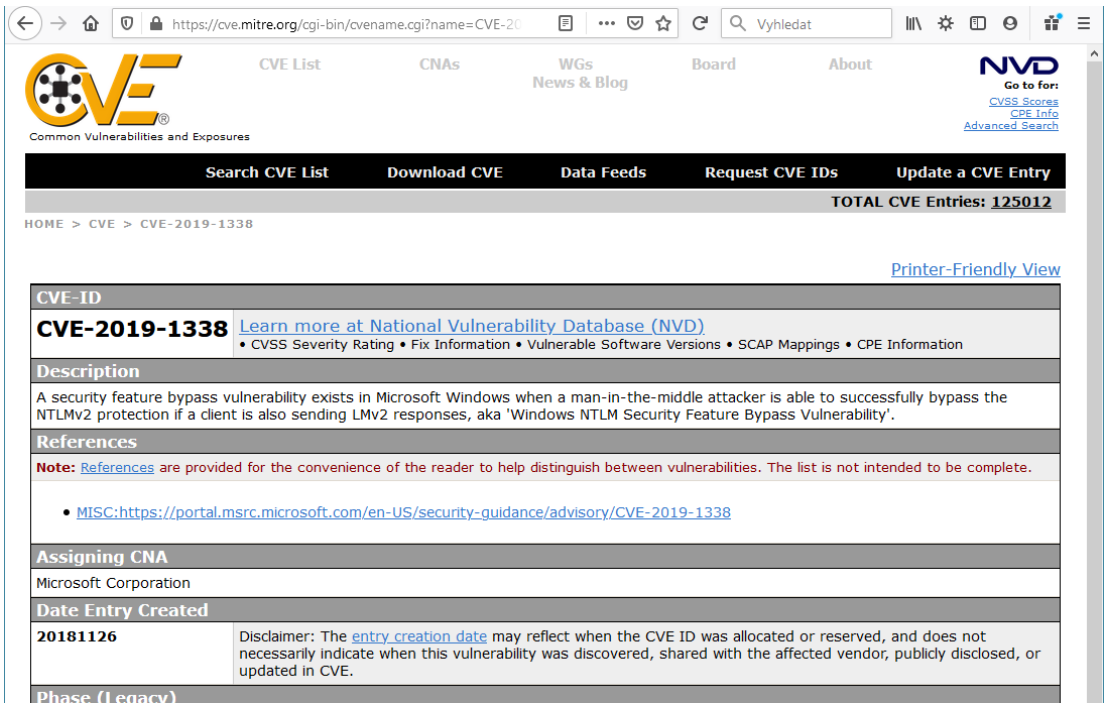
Většina malwaru se do systému dostává takto:

- využitím bezpečnostních nedostatků (bezpečnostních děr, zranitelností) v operačním systému a knihovnách, které poskytuje,

- využitím bezpečnostních děr v aplikacích nebo jejich knihovnách,
- jinými způsoby – v e-mailu (obvykle spíše jeho příloze), přes různé komunikátory (Skype apod.), využitím zranitelností na webových stránkách, které uživatel navštěvuje, z výměnných paměťových médií (infikovaný USB flash disk), přes špatně zabezpečené síťové rozhraní, atd.

Třetí možnost je vlastně speciálním případem prvních dvou, protože i tak ve skutečnosti jde o selhání konkrétní aplikace nebo nedostatek obezřetnosti firewallu či antiviru (což jsou taky aplikace).

Pokud je objevena bezpečnostní mezera v softwaru, měl by se to především dozvědět producent toho softwaru (například pokud jde o bezpečnostní chybu v Adobe Acrobatu, měla by být informována společnost Adobe). Ne vždy tomu tak je. Bohužel existují lidé, kteří s objevenými zranitelnostmi obchodují na černém trhu. Velké společnosti se tomu snaží předejít odměnami za nahlášené bezpečnostní mezery, přičemž čím víc zneužitelná je tato mezera, tím vyšší částka je vyplacena.



Obrázek 1.1: CVE záznam

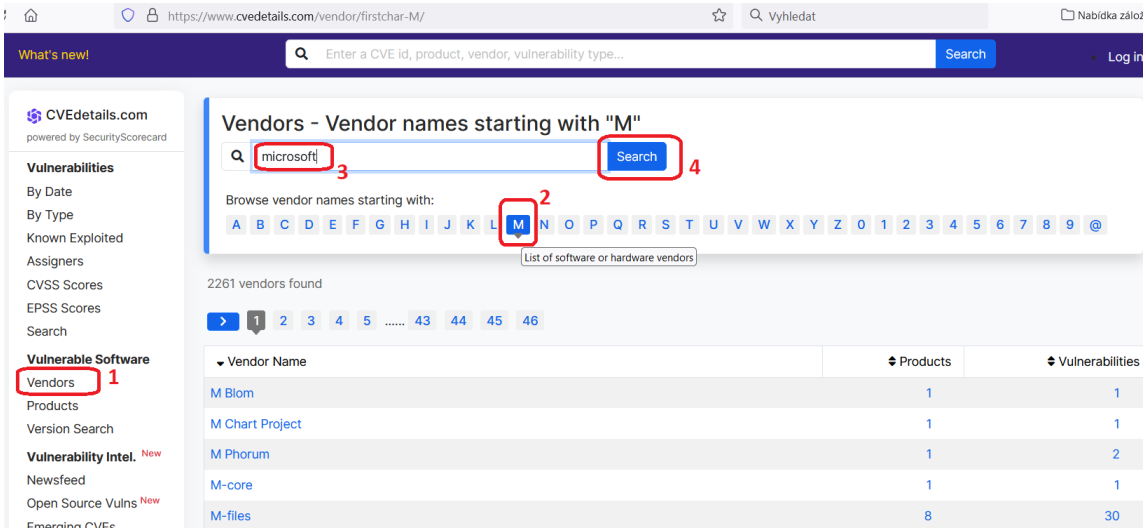
Aby byl v seznamech zranitelností pořádek, jsou ukládány v jednotném formátu – *CVE* (Common Vulnerabilities and Exposures). Formát CVE se používá obecně všude, aby si příslušné aplikace a weby mohly tyto informace jednoduše předávat.

Na obrázku 1.1 je výpis CVE záznamu pro zranitelnost s kódem „CVE-2019-1338“. Tato zranitelnost v MS Windows umožňuje obejít autentizační proces při přístupu přes počítačovou síť.

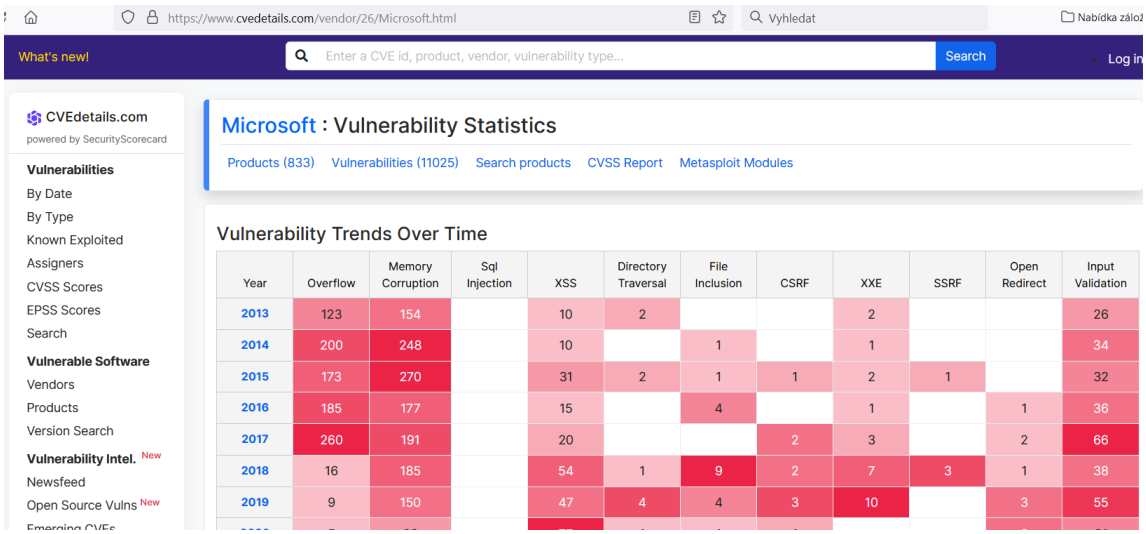
Správcem CVE databáze je společnost Mitre, na jejím webu (https://cve.mitre.org) se k této databázi taky dostaneme (na obrázku vidíme odkazy „Search CVE List“, „Download CVE“). Existují i další databáze zranitelností, ovšem všechny tyto databáze navzájem spolupracují, jen v některých můžeme najít více podrobností. Například na obrázku 1.1 vidíme odkaz do databáze NVD vedené organizací NIST.

K položkám databáze CVE vedené organizací Mitre se dostaneme i na https://www.cvedetails.com. Je to jen jiná cesta k téže databázi, ale pro někoho může být zajímavější – nabízí i statistiky a grafy.

Na obrázku 1.2 je naznačen přístup k zranitelnostem produktů Microsoftu. V menu vlevo zvolíme *Vendors*, pak se ve vyhledávání postupně dostaneme k Microsoftu, potvrdíme. Výsledek hledání je na obrázku 1.3. Nejdřív získáme obecné statistické informace včetně počtu různých typů zranitelností nalezených v produktech daného výrobce, po klepnutí na rok nebo pole v tabulce se dostaneme na seznam příslušných zranitelností.



Obrázek 1.2: Přístup k databázi CVE Details

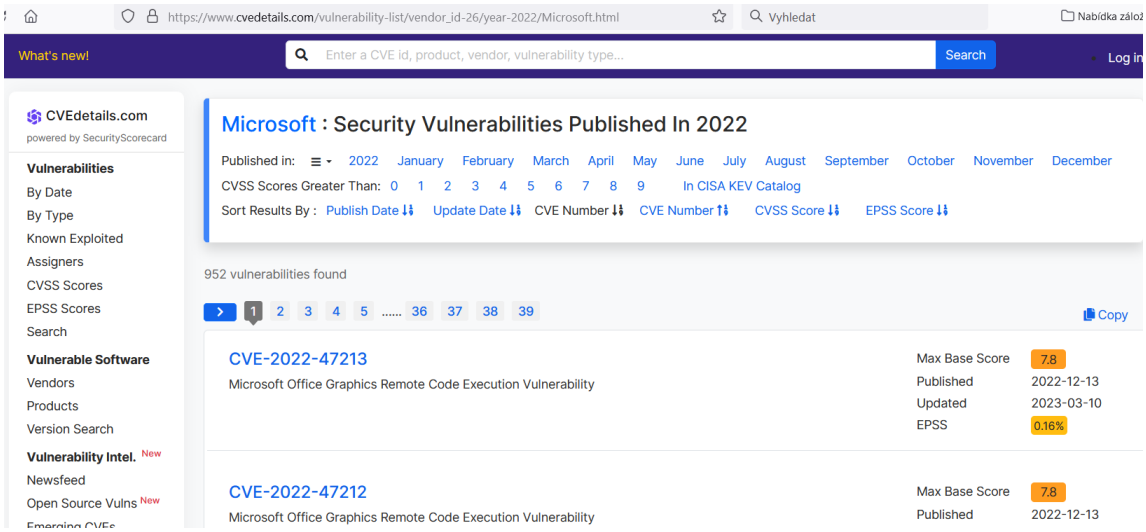


Obrázek 1.3: CVE Details, údaje produktech Microsoftu

Na následujícím obrázku je seznam zranitelností v produktech MS nalezených v roce 2022: přímo na této stránce máme ke každé zranitelnosti základní informace, k podrobnostem se dostaneme po vybrání konkrétního záznamu.

Bezpečnostní mezery typu „Zero day“ (den nula) jsou takové, pro které ještě neexistuje záplata (obvykle proto, že ještě nebyly zjištěny producentem softwaru, ale hackery ano). Proti těmto mezerám aktualizace nepomohou, ale může pomoci aktualizovaný antimalwarový software.

Seznamy zranitelností nejsou jenom na webu, také existují nástroje, které dokážou proskenovat



Obrázek 1.4: CVE Details, seznam zranitelností v produktech Microsoftu nalezených v roce 2022

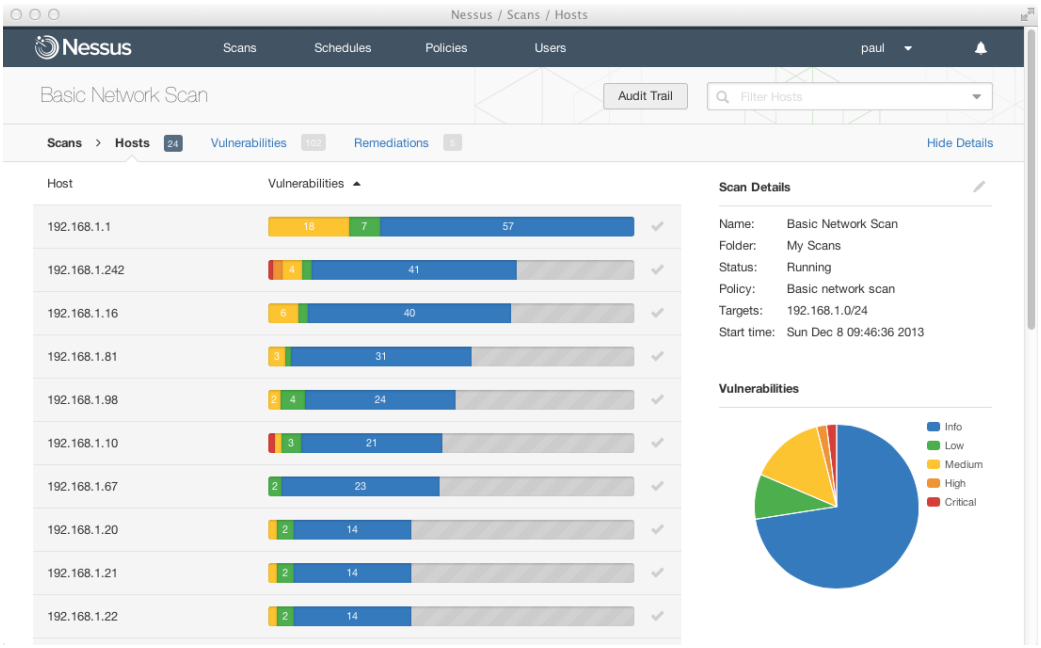
počítače v místní síti a pro každý zobrazit seznam nalezených zranitelností. Je to praktičtější než pravidelně sledovat web, jestli tam nepíšou něco o našem systému či aplikaci. Takový nástroj používá databázi zranitelností (vulnerability database) s CVE záznamy dosud známých zranitelností, plus záznamy o obvyklých bezpečnostních „nešvarech“ v konfiguraci různých operačních systémů a aplikací. Po spuštění vyhledá v síti připojená zařízení a na každém spustí testování. Obvykle pro testovaná zařízení předem zadáváme přihlašovací údaje (credentials), aby se nástroj na dané zařízení „dostal“ a mohl prověřit systém důkladněji, ale lze provádět testování i bez přihlašovacích údajů (pak by získané údaje odpovídaly tomu, k čemu by měl přístup případný útočník – black box testing).

Takových nástrojů existuje více, například:

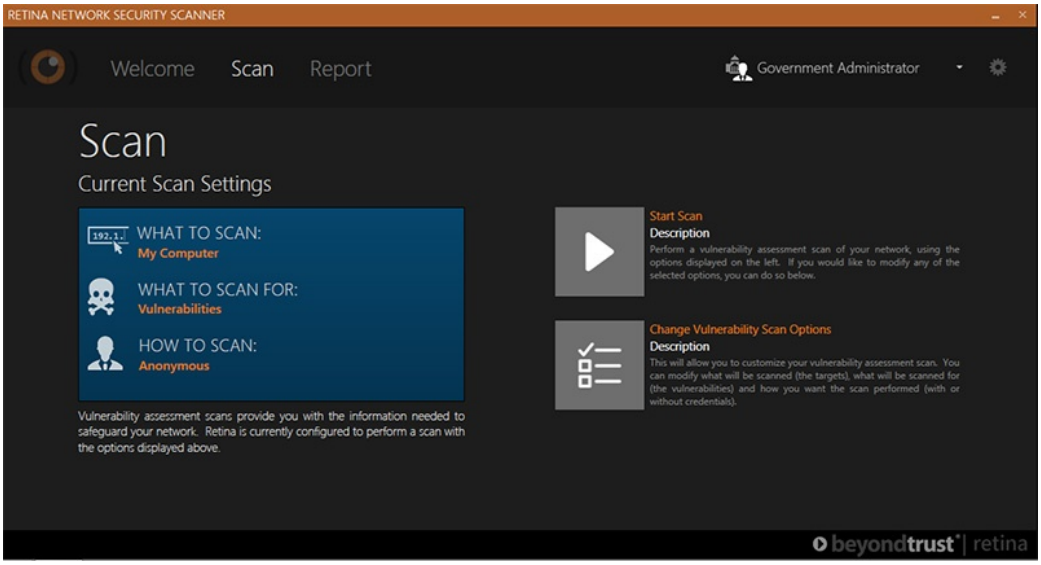
- *Nessus* (https://www.tenable.com/products) je jeden z nejznámějších bezpečnostních scannerů, edice Home je pro nekomerční použití zdarma, webové rozhraní nástroje vidíme na obrázku 1.5.
- *Retina* (https://www.beyondtrust.com/products/retina-network-security-scanner/) je na rozdíl od jiných (ovládajících se přes webové rozhraní) naprogramována jako aplikace a má také zdarma dostupnou komunitní edici. Rozhraní vidíme na obrázku 1.6.
- *Nexpose* (https://www.rapid7.com/products/nexpose/) má také komunitní edici, ale oproti jiným nástrojům má také velmi vysoké hardwarové nároky.
- *OpenVAS* (http://www.openvas.org/) je jako jediný plně volně šiřitelný (nemá žádnou komerční edici) a je distribuován pod svobodnou licencí, ale pro jeho provoz potřebujeme Linux (ovšem pokud nabootujeme Kali Linux, máme už OpenVAS k dispozici, nemusíme nic instalovat).
- *GFI LanGuard* (http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard) je čistě komerční produkt, ale máme možnost si ho vyzkoušet v trial verzi.

Poznámka:

Těmito nástroji si můžete otestovat i vlastní domácí síť. Stačí spustit na počítači připojeném do sítě, zadat potřebné údaje a nechat pracovat.



Obrázek 1.5: Bezpečnostní scanner Nessus (rozhraní)[1]



Obrázek 1.6: Bezpečnostní scanner Retina (rozhraní)[2]

Další informace:

Všechny výše uvedené nástroje jsou otestovány a srovnány v diplomové práci Masnica, Bořivoj. *Nástroje pro automatické vyhledávání bezpečnostních mezer*, diplomová práce. Slezská univerzita v Opavě: 2016.

[1] Zdroj: https://www.tenable.com
[2] Zdroj: https://www.beyondtrust.com

1.2 Automatické aktualizace systému

Existence bezpečnostních problémů se ani zdaleka netýká jen Windows. Každý operační systém (Windows, Linux, MacOS) dnes nabízí možnost automatických aktualizací, jistý systém ani nedává běžnému uživateli možnost s nimi „nesouhlasit“.

Pro kritické zranitelnosti platí, že záplata by měla být k dispozici co nejdřív. U ostatních se naprogramování záplaty nechává na dobu „až je čas“, nebo (v případě Windows) na tzv. „Patch Day“ (den záplat) – vždy druhé úterý v měsíci.

Ve všech dnes běžných operačních systémech pro desktopy a notebooky existuje určitá automatizace instalace aktualizací, tj. uživatel je upozorněn na existenci aktualizace a požádán o povolení její instalace, případně je aktualizace bez jakéhokoliv souhlasu nainstalována (což je výchozí pro Windows).

U mobilních zařízení situace není ani zdaleka tak jasná. Produkty od společnosti Apple a Microsoft fungují v podobném režimu, jaký je popsán výše, ale zařízení s Androidem bohužel na většinu aktualizací nedosáhnou. Je to proto, že Android běží na velkém množství různorodých zařízení a je vždy na výrobci takového zařízení, jestli aktualizaci adaptuje (přizpůsobí) a distribuuje na příslušná zařízení.

Za určitých okolností může nastat situace, kdy po instalaci aktualizací systému přestane správně fungovat některé zařízení nebo aplikace. Důvod je obvykle v tom, že aktualizace zasáhne do některé knihovny (v případě nefunkčnosti aplikace) nebo do systému správy ovladačů (v případě nefunkčnosti zařízení). V takovém případě může pomoci

- restart systému (například tehdy, když kurzor po restartu nereaguje na pohyb myši),
- návrat v konfiguraci (vrátíme změny provedené aktualizací). Ve Windows k tomu můžeme použít nástroj Obnovení systému.

Nejhorší situace nastává, když systém po aktualizaci odmítá startovat. Pak nezbývá než se pokusit systém spustit alespoň v nouzovém režimu a tam vrátit změny provedené aktualizací.

Poznámka:

Uživatelé jsou často překvapeni tím, kolik bezpečnostních děr je v systému a aplikacích. Bohužel platí, že čím složitější systém, tím větší je pravděpodobnost, že se v něm něco takového objeví. U velmi složitých systémů s mnoha řádky kódu, na kterých spolupracuje celý tým lidí, je prakticky nemožné se těmto problémům vyhnout, a aktualizace jsou nezbytné.

1.3 Aktualizace aplikací

Z bezpečnostního hlediska jsou důležité také aktualizace aplikací. Může totiž dojít ke zneužití některých „vedlejších efektů“ běhu aplikací. Jsou potřebné prakticky u všech větších aplikací, a kriticky potřebné zejména u těch, které pracují se soubory či jakýmkoliv „cizím“ vstupem: webové prohlížeče, dále Adobe Reader, Adobe Acrobat, Flash Player, Apple QuickTime, obecně také nejrůznější přehrávače multimediálních souborů a kancelářské aplikace (včetně MS Office a OpenOffice.org).

Nejobvyklejší způsob zneužití aplikace je *přetečení paměti* (buffer overflow). Buffer je paměťový prostoru procesu, do kterého si proces ukládá svá data a další potřebné informace. Proces je donucen uložit na dané místo více, než kolik se tam vejde, a pak tedy dochází k zápisu dat (nebo čehokoliv

jiného) za vymezené hranice. Důsledkem může být „jen“ chybné chování programu či jeho pád, ale také zápis nebezpečných dat (případně instrukcí kódu) tam, kde nemají co dělat.

Buffer overflow se většinou týká jednoho typu bufferu, který nazýváme zásobník (stack), jde tedy o *stack overflow* (existuje také přetečení haldy – heap overflow). Každý proces má obvykle dva zásobníky (jeden pro uživatelský režim, druhý používá jádro při obsluze požadavků tohoto procesu), do kterých se ukládají informace o momentálně běžících funkcích (aktivační záznamy – skutečné parametry funkce, lokální proměnné, také *adresa instrukce následující po instrukci, která tuto funkci zavolala*, atd.). Přetečení zásobníku funguje tak, že proces „omylem“ zapisuje data mimo část paměti určenou pro zásobník, tam, kam se zapisuje něco zcela jiného. To samo o sobě může způsobit chybné chování či pád aplikace, ale následky mohou být mnohem horší, včetně přepisu instrukcí procesu (takže potom se může stát, že jsou zpracovávány jiné instrukce než by měly).

Jak bylo výše naznačeno, v zásobníku je u každého aktivačního záznamu uložena adresa instrukce následující po té, která dotyčnou funkci zavolala. Tento údaj je pro proces důležitý, protože mu říká, kde pokračovat po dokončení volané funkce. Pokud uloženou adresu přepíšeme jinou (podstrčenou) adresou (a případně upravíme část paměti v cíli této adresy), důsledkem je spuštění jiného kódu, než jaký se správně měl dále provádět. Spuštěný kód může být rovněž podstrčený, často bývá ukryt ve speciálně navržených datech. Podstrčenému kódu se říká *shellcode*.

Funkce, kterou třeba v případě Windows nazýváme *Zabránění spuštění dat* (DEP), dělí stránky paměti procesu na ty, kde jsou instrukce (executive), a ty, kde jsou data (datové, non-executive). Pokud se proces pokusí zacházet s něčím na datové stránce jako s instrukcí (tj. to, co by mělo být např. číslo, pošle procesoru jako instrukci k provedení), je to považováno buď za vážnou chybu, nebo za pokus spustit podstrčený kód, a proces je okamžitě ukončen. Kód mohl být podstrčen například pomocí buffer overflow.

Funkce DEP může být implementována buď hardwarově, nebo softwarově. Hardwarová implementace využívá vlastnost procesorů společností AMD a Intel – NX bit (Non-executive; u Intelu XD bit, Execute-disable), která umožňuje označit paměťové stránky jako čistě datové. Softwarová implementace je pouze na straně operačního systému, používá se, když procesor „neumí“ NX/XD bit. 64bitové systémy používají výhradně hardwarovou implementaci.

Ve všech dnes běžných operačních systémech kromě Windows tato funkce běží nativně a není nutné ji jakkoliv konfigurovat. Ve Windows platí totéž pro hardwarovou implementaci. Ovšem softwarová implementace (když hardwarová není k dispozici) je pouze pro důležité systémové programy a služby, případně se některé z nich dají „vyjmout“, konfiguruje se v nástroji *Systém*, *Upřesnit nastavení systému*, karta *Upřesnit*, v horní části tlačítko *Nastavení*. Dá se zapnout pro procesy – v nástroji *Emet*.[3]

Jak se bránit rizikům spojeným se spouštěním podvrženého kódu?

1. Aktualizovat aplikace, případně sledovat zveřejňované informace o problémech. V aktualizacích (či nových verzích) bývají často odstraňovány chyby typu přetečení zásobníku.
2. Dávat pozor, co otevírám; ne vše, co přijde e-mailem, stojí za otevření.
3. Programátoři by měli používat tzv. bezpečné programování, které má tyto problémy eliminovat.

Poznámka:

Za určitých okolností je možné, že se podstrčený kód spustí i v případě, že upravený soubor neotevřeme.

[3] Emet je ke stažení na https://www.microsoft.com/en-us/download/details.aspx?id=50766

Před časem (publikováno v Chip 6/09, str. 24) byla objevena chyba v Adobe Readeru a Adobe Acrobatu (konkrétně v Adobe PDF-Parseru), která právě to umožňuje. Pokud je napadený PDF soubor uložen na disku a nalezen službou *Indexing service*, tato služba se pokusí ho zařadit do indexu včetně klíčových slov z jeho obsahu. Aby se dostala k textu v souboru, používá parser, který (neúmyslně) spustí kód uložený v podstrčeném souboru. Problém je v tom, že služba Indexing service běží s administrátorskými právy, která zdědí také spuštěný podstrčený kód. Ve verzích od 9.1 je tato chyba již odstraněna.

Co se internetových prohlížečů týče, již dlouho se diskutuje o zabezpečení před chybami zásuvných modulů (pluginů). Týká se to především pluginu Macromedia Flash od společnosti Adobe, který je všeobecně znám svými bezpečnostními nedostatky, a implementace programovacího jazyka ActionScript (v něm se programují především flashové animace). Pluginy se totiž konfigurují zvlášť a nepřebírají mnohá globální nastavení, o kterých předpokládáme, že by měla platit pro prohlížeč jako celek. Důsledkem těchto úvah je, že v některých prohlížečích či systémech již Flash soubory vůbec nelze přehrát (bojkot), a flash animace jsou na webu postupně nahrazovány animacemi v HTML5.

Úkol

Prověřte bezpečnostní výbavu počítače, u kterého sedíte – zda je operační systém aktualizovaný, který antivirus je nainstalován (a případně další bezpečnostní software), zda je aktuální.

1.4 Hesla

Mnozí uživatelé pracují na počítači bez hesla nebo se snadno uhádnutelným heslem. Pokud se navíc jedná o heslo k účtu s administrátorskými právy, jedná se o dost nebezpečné chování. Hesla by měla být sice zapamatovatelná, ale nesnadno uhádnutelná (například vytvoříme dostatečně dlouhý řetězec poskládaný z několika řetězců, které si dokážeme snadno zapamatovat, a pak třeba přehodíme několik znaků a přidáme pár takových, které nejsou písmeny – číslice, otazník, závorky, čárka apod.).

Zatímco heslo, které je vlastně jen běžným slovem, lze prolomit za méně než sekundu, silné heslo (dostatečně dlouhé a složité) odolá výrazně déle (i celá léta výpočetního času).

Pro prolamování hesel se nejvíc používají dva typy útoků:

- *slovníková metoda* – proces má přístup k seznamu slov, která by mohla být použita jako heslo,
- *metoda hrubé síly* (Brutal Force) – proces generuje různé řetězce a dosazuje je (omezíme vyhledávání například na hesla o délce 3–8 znaků, určíme, zda se tam pravděpodobně budou vyskytovat i jiné znaky než písmena, apod.).

Pokud se jedná o hesla do systému nebo hesla k různým (webovým) službám, obvykle se ukládají pouze ve formě *hashe* (obdoby kontrolního součtu, taky „otisk“), tedy krátkého řetězce, který neobsahuje samotné heslo, ale vznikl použitím jednocestné hash funkce na toto heslo. Hash funkce jsou jednocestné, tj. z hesla vyrobíme jeho hash, ale naopak to nejde (z hashe nedostanete původní heslo), protože při převodu hesla na hash se část informace ztrácí. Zároveň platí, že stačí i jen malá změna v původním řetězci (hesle), a hash se změní velmi výrazně.

Jestliže se hackerovi podaří dostat k souboru s hashi hesel a ví, který hashovací algoritmus byl pro vytvoření hashů použit, může použít stejný typ útoku jako na skutečná hesla (přičemž na heslo vybrané ze slovníku či vygenerované použije hash funkci a výsledek pak porovnává se záznamy v souboru), nebo

může mít předpřipravenou obdobu slovníku obsahující k heslům i jejich hashe, což mu šetří práci. Tabulky se seznamy hashů hesel se nazývají *Rainbow Tables* (duhové tabulky).

Windows si hashe hesel ukládají do části registru, která není uživatelům přístupná (v klíči `SAM`). V systémech UNIXového typu se pro tento účel používá soubor `/etc/shadow`, taktéž běžným uživatelům nedostupný. Samotná hesla nejsou nikde ukládána, takže ani nemá smysl žádat někoho, aby ze systému „vytáhl heslo“. Nicméně heslo se dá (u Windows) resetovat, tedy zaměnit za jiné (popřípadě prázdné).

Poznámka:

Pokud zapomenete heslo k webové službě a máte možnost požádat o jeho zaslání (třeba e-mailem), pak zpozorněte – adminitrátor té služby má k dispozici hesla a nikoliv jen hashe? Správně a bezpečně by nastavení hesla mělo probíhat tak, že šifrovaným kanálem pošlete heslo, systém z něj vypočte hash, uloží ho a původní heslo zlikviduje. Kdykoliv se pak znovu přihlašujete, přijme heslo šifrovaným kanálem, vypočte z něj hash, porovná ho s uloženým hashem a zaslané heslo opět zlikviduje (zapomene).

Pokud má (jakýkoliv) systém k dispozici přímo hesla, pak je dost možné, že ani jiná bezpečnostní opatření nebudou zrovna na výši, a pravděpodobnost odcizení hesel je vysoká.

Jaká je alternativa k „připomenutí“ přímo hesla? E-mailem můžete dostat odkaz, přes který můžete své heslo resetovat (nahradit jiným), takže to původní nebudete potřebovat.

Pokud hackeři odcizí soubory s hesly, mohou je okamžitě začít zneužívat, ale pokud odcizí soubory s hashi hesel, musejí podstoupit dlouhou cestu postupného prolamování hesel třeba slovníkovou metodou (vezme se řetězec, vypočte se jeho hash, porovná se se získaným hashem, když nesedí, vezme se další řetězec,...). Navíc hash funkcí existuje víc, hackeři musejí zkoušet nejen slova, ale i různé hash funkce.

Úkol

Máte silné heslo? Pokud ne, nějaké vymyslete (takové, které by bylo zároveň zapamatovatelné).

Určitou pomocí jsou *správci hesel*. Bohužel ne vždy je tato možnost zcela bezpečná, protože právě na správce hesel útočí hackeři obzvlášť zuřivě (čím zajímavější „náplň“, tím větší lákadlo, a hesla jsou velmi zajímavá). Pokud se pro nějakého správce hesel rozhodneme, pak bychom měli zvážit, jestli opravdu chceme mít hesla v cloudu (aby byla přístupná pro všechna vlastní zařízení). Je to sice pohodlnější, ale méně bezpečné. K nejznámějším správcům hesel patří:

- Sticky Password (český produkt) – https://www.stickypassword.com/cs/,
- LastPass – https://lastpass.com/,
- Bitwarden – https://bitwarden.com/,
- 1Password – https://1password.com/,
- KeePass – https://keepass.info/,
- Steganos Password Manager – https://www.steganos.com/en/products/steganos-password-manager.

V každém případě alespoň jedno heslo máme – ke správci hesel. Ten pak uchovává a případně i na webech předvyplňuje ostatní hesla. Heslo ke správci by mělo být dostatečně silné, ale zároveň zapamatovatelné.

1.5 Sociální inženýrství

Sociální inženýrství je metoda, jak z uživatele vytáhnout potřebné informace třeba i bez použití techniky, a to jeho uvedením v omyl (obelstěním). Uživatel je přesvědčen, že informace předává důvěryhodné osobě z naprosto nutných důvodů.

Útočník se vydává například za zaměstnance bezpečnostního oddělení, opraváře, zaměstnance telefonní společnosti, nového kolegu apod. a nenápadně ze svých obětí vytáhne vše potřebné, obhlédne místa, kde si lidé lepí papírky s hesly, případně si „vyzkouší“ nový skvělý počítač nebo se jinak dostane k technice na pracovišti. Stává se to především ve větších firmách, kde se nepočítá s tím, že by se všichni zaměstnanci znali, ale kontakt může probíhat i „neosobně“ přes telefon nebo e-mail. Právě do telefonu jsou zaměstnanci schopni říci neuvěřitelné věci včetně těch, které jsou obchodním tajemstvím.

Sociální inženýrství může mít i „materiální“ povahu – například volně „pohozená“ přenosná zařízení, která jsou pro mnoho lidí neodolatelná. Podle DHS[4] je kolem 60 % běžných uživatelů schopno náhodně nalezený USB flash disk připojit ke svému počítači, třebaže netuší, zda se na něm nenachází škodlivý software. Podobně lze zneužít i jiná přenosná zařízení, zde je nejlepší ochranou poctivost, tedy odevzdat nalezený předmět do ztrát a nálezů.

Poznámka:

Sociální inženýrství je v současné době jedna z nejpoužívanějších (a taky nejefektivnějších) metod získávání utajených informací. Na to by měli myslet zejména administrátoři firemních sítí a zajistit patřičné školení všech, kdo se do firemní sítě připojují. Tento typ útoku získává nový rozměr také v souvislosti se sociálními sítěmi (jak ve firemním prostředí, tak i soukromě). Na sociální síti lidé „vybreptají“ mnohem víc zneužitelných informací, než si sami připouštějí.

Postup

Jak se bránit?

- Heslo či jiné podobné údaje si nenecháváme na papírku přilepeném k monitoru, pod klávesnicí, na tiskárně (nebo na jiných „obvyklých“ místech). Volíme silná hesla.
- Nevěříme všemu, co kdo povídá. Zvláště když jsem například administrátor firemní sítě, musím si vše ověřovat (totožnost žadatele o nové heslo po jeho zapomenutí, nutnost provedení požadovaného zásahu do systému, apod.).
- Správce sítě by měl mít každou žádost o zásah do účtů zaměstnanců nebo systému vždy „papírově“ či jinak podloženou.
- Každý systém zabezpečený heslem (včetně operačních systémů) lze nastavit tak, aby po stanoveném počtu chybných pokusů o přihlášení byl účet zablokován. Právě proto nám třeba u bankomatu stačí krátký „slabý“ PIN kód, útok hrubou silou je zastaven už po několika pokusech.
- Banky ani jiné instituce nechtějí po svých klientech zasílání hesel, certifikátů, TAN, čísla kreditní karty a podobných údajů e-mailem ani žádným jiným nezabezpečeným způsobem (jen přes šifrované stránky přímo při přihlašování). A rozhodně o ně nežádají e-mailem ani telefonem.
- Neprovozujeme bezhlavé klikání na odkazy uvedené v e-mailech, radši si ověříme, kam konkrétně vedou, případně zkopírujeme celou adresu do webového prohlížeče.

[4] DHS (Department of Homeland Security, http://www.dhs.gov)

- Pokud zahlédneme pohozený USB flash disk či podobné zařízení, radši si ho nevšímáme nebo zaneseme na nejbližší místo, na které se vracejí věci (například na Informace, recepci, helpdesk apod.). Rozhodně takové zařízení nepřipojujeme ke svému počítači, případné nákazy bychom si ze začátku vůbec nemuseli všimnout.
- Útočníci používající sociální inženýrství dělají „domácí úkoly“ – shánějí co nejvíc informací (včetně osobních), které by mohli využít. Firma by měla zvážit, co zveřejní (a totéž platí i o domácích uživatelích, také například na diskusních fórech a sociálních sítích).

Kapitola 2

Malware

Malware (malicious software – záludný, škodlivý software) je souhrnný název pro různé typy škodlivého kódu. Nejčastější typy malwaru jsou trojské koně, viry, červi, spyware a další. Zatímco dřív se vyskytovaly téměř výhradně škodlivé kódy pro Windows, v poslední době narůstá množství malwaru pro mobilní platformy, zejména OS Android.

Rychlý náhled: V této kapitole postupně probereme různé druhy malwaru – spam, trojské koně, viry, atd., ke každému je zde uvedena jeho charakteristika a většinou také příklady známých „kusů“. Poslední sekce se věnuje botnetům.

Klíčová slova: Malware, spam, trojský kůň, virus, červ, spyware, rootkit, ransomware, backdoor, phishing, pharming

Cíle studia: Po prostudování této kapitoly se naučíte rozlišovat různé typy škodlivého softwaru a jeho projevy.

2.1 Malware podle toho, jak se k nám dostane

2.1.1 Virus

Virus je takový škodlivý kód, který ke své existenci potřebuje nějaký nosič: existující kód (obvykle spustitelný soubor) – virus takový kód „nakazí“. Je to podobné jako u biologických virů. Aktivovat se nedokáže sám, ale musí počkat, až jeho nosný program bude spuštěn.

Virus se dokáže sám množit, a to takto: pokud je jeho nosný program spuštěn, prohledá dostupné zařízení, hledá takové soubory, se kterými si dokáže poradit (mohou to být spustitelné soubory, třeba ve Windows s příponou exe, nebo například dokumenty používající makra). Každý takový „vhodný“ soubor upraví: do spouštěcí sekvence přidá sám sebe, svůj vlastní kód, čímž zajistí, že při spuštění souboru bude proveden také kód viru.

Antivirové programy původně rozlišovaly viry od běžných programů pomocí virových signatur. *Virová signatura* je řetězec, který jednoznačně identifikuje program napadený konkrétním virem, může jít například o hash určité části kódu (té inicializační části, která byla zmíněna výše). Antivirus používající tuto základní metodu jednoduše prohledává soubory a hledá v nich úsek odpovídající signatuře.

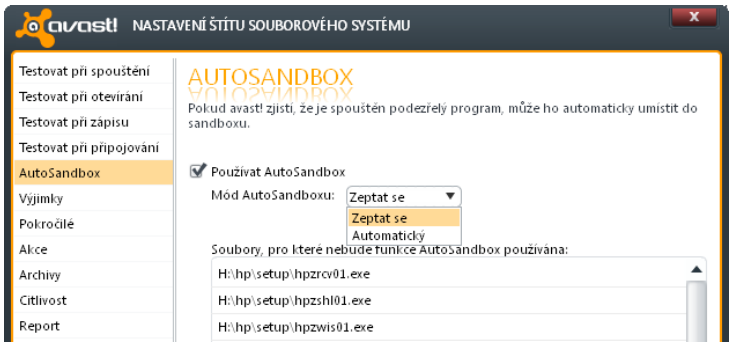
Aby se prohledávání urychlilo, antiviry zkoumají soubory z více hledisek (také například typ souboru) a prohledávají jen tu část souboru, ze kterých se signatura obvykle počítá.

Antivirovým společnostem zamotaly hlavu tzv. *polymorfní viry*. Tyto viry dokázaly odolávat tehdejším virovým skenerům tak, že často modifikovaly samy sebe (při svém množení, vytváření svých kopií) a znemožňovaly identifikaci pomocí virových signatur. Modifikace většinou spočívala ve změně způsobu kódování programu – tatáž akce se dá provádět (kódovat) více různými způsoby, případně dotyčný kód mohl být různým způsobem komprimován (jako například v ZIP souborech).

Současné viry jsou prakticky vždy polymorfní, mění svůj kód a jeho strukturu při téměř každém duplikování, takže signatury je třeba často aktualizovat, a ani to nepomáhá (je třeba použít jinou metodu).

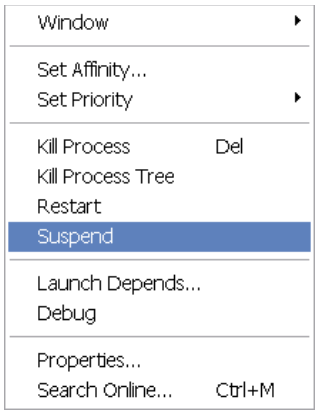
Detekce pomocí signatur už dnes není považována za dostačující. Sice se pořád používá, ovšem nefunguje nejen na polymorfní a metamorfní viry, ale ani na tzv. *zero-day útoky* (tj. útoky zneužívající zranitelnosti, které zatím objevili jen hackeři, tj. zero-day zranitelnosti). Zde jsou úspěšnější spíše jiné metody: heuristiky a detekce podezřelého chování, tyto metody jsou vysvětleny v následující kapitole.

K detekci virů se používají také emulátory (chráněné prostředí, ve kterém se podezřelý program spustí a zkoumají se jeho reakce). Emulace je poměrně náročná metoda detekce (asi nejznámější metoda je tzv. *SandBox* – „píseček“). Výpočetní náročnost emulace je obvykle řešena tak, že proces běží v emulátoru pouze po omezenou dobu, po které již může pracovat běžným způsobem. V prostředí antiviru bývá obvykle možné funkci sandboxu konfigurovat, příslušné okno z programu Avast! vidíme na obrázku 2.1.



Obrázek 2.1: Konfigurace sandboxu v programu Avast!

Za určitých okolností může virus „poznat“, že běží v emulátoru. Reakcí na tuto obranu jsou *metamorfní viry*, které se dokážou chránit i před odhalením emulací.



Obrázek 2.2: Suspendování procesu

Ke známým obranným mechanismům virů také patří vzájemné hlídání procesů. Virus má spuštěno více procesů, které se navzájem hlídají; pokud zjistí, že některý z těchto procesů byl ukončen, znovu ho spustí.

Tento problém se řeší postupným uspáváním těchto procesů (suspend, na obrázku 2.2 vidíme kontextové menu procesu v aplikaci Process Explorer od Sysinternals s právě touto položkou vyznačenou), až potom mohou být všechny tyto procesy ukončeny (žádný z nich po suspendování vlastně nehlídá), pro jistotu ukončujeme i případné potomky tohoto procesu (tj. jeho podstrom). To ovšem funguje pouze tehdy, pokud se nám podaří odhalit všechny „spolupracující“ procesy. Jestli jsme na některý proces zapomněli, zjistíme to velmi rychle – ukončené procesy budou za chvíli zpět.

Poznámka:

Pokud se virus dostane do složky `System Volume Information` a napadne body obnovy, je třeba vypnout funkci *Obnovení systému* a smazat všechny body obnovy (nebo jen napadené, pokud je rozeznáme), aby se z těchto záloh virus po odstranění nedostal zpět do systému.

Příklad

V roce 2022 se rozšířil virus FluBot. Tento virus cílí na mobilní zařízení a šíří se překvapivě pomocí SMS a MMS na zařízeních s OS Android. Uživateli přijde zpráva, ve které je přesvědčován, že má ve schránce hlasovou zprávu a pro její otevření musí kliknout na přiložený odkaz. Po kliknutí je nabídnuta instalace aplikace, která si s danou úlohou „poradí“, ovšem ve skutečnosti je nainstalován škodlivý kód, který okamžitě načte seznam kontaktů a na všechny rozešle podobnou SMS či MMS zprávu.

2.1.2 Trojský kůň

Trojský kůň (trojan) je škodlivý program (obecně kód), který předstírá, že jde o něco úplně jiného. Jde buď o (klasické) podstrčené či pozměněné programy (dokonce i náhrady systémových programů nebo spořiče obrazovky).

Rozdíl mezi virem a trojanem je v tom, že zatímco virus nakazí nějaký existující (původně užitečný) program, trojan si vystačí sám: samotný trojan je programem, který se tváří užitečně. Podobně jako virus, také trojan nechává svou aktivaci a tím i šíření na uživateli.

Trojské koně se do systému dostávají buď e-mailem (nemusí jít jen o spam), může jít o soubor stažený přes webový prohlížeč z internetu či jiného zdroje, trojanem může být systém nakažen i z infikovaného přenosného média. Dokonce se vyskytly případy, kdy byl napaden aktualizační server jisté firmy a místo jedné aktualizace byl podstrčen trojan, ale aktualizační servery jsou dnes naštěstí obzvlášť pečlivě chráněny.

Příklad

Trojan *ZuoRAT* (objevený v roce 2022, ale působící v té době už alespoň dva roky) napadá routery různých výrobců a ovlivňuje veškerá zařízení k nim připojená metodou vzdáleného přístupu (zvládá zařízení s Windows, MacOS, Linuxem). ZuoRAT zneužívá bezpečnostní zranitelnosti v softwaru routeru, tato zařízení totiž většina uživatelů neaktualizuje. Naštěstí tento malware není schopen přežít restart zařízení, nicméně i po restartu po sobě zanechává stopy (těch se dá zbavit jen přechodem do továrního nastavení).

https://www.zive.cz/clanky/malware-zuorat-infikuje-routery-cisco-netgear-asus-a-daytek-a-spehuje-sitovy-provoz/sc-3-a-217244/default.aspx

ZuoRAT není prvním malwarem, který napadl velké množství routerů a dalších zařízení od různých výrobců. Roku 2018 to byl červ VPNFilter (což zní poměrně nevinně), který byl zjištěn na nejméně půl milionu routerů (celkové množství napadených zařízení je zřejmě mnohem větší). FBI považuje za původce červa VPNFilter ruskou skupinu Fancy Bear. VPN Filter se bohužel až tak jednoduše nedá odstranit (dočasnou pomocí je také restart routeru), ale FBI se podařilo zlikvidovat většinu serverů, na

které se napadená zařízení napojovala, což omezilo škodlivost dotyčného softwaru.

https://www.trendmicro.com/en_vn/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

Příklad

INF/Autorun je trojský kůň, který se integruje do souboru `autorun.inf` na výměnném paměťovém médiu (oblíbil si zejména USB flash disky, které jsou velmi používané). Tento soubor nemusí být viditelný, může mít nastaven atribut „skrytý“. Jde o metodu šíření, která je používána různými typy malwaru, zejména červy (také Conficker ji svého času používal).

Soubor `autorun.inf` se standardně spouští při každém připojení paměťového média a za normálních okolností obsahuje například odkaz na webovou stránku, která se má otevřít, program, který má být spuštěn nebo obecně zajišťuje provedení nějaké akce při připojení média. Jde o velmi běžný typ malwaru především z důvodu snadné rozšiřitelnosti (funkce automatického spouštění obsahu pro výměnná paměťová média je na téměř všech počítačích zapnuta). Pokud připojíme k počítači infikované paměťové médium, okamžitě se nakazí.

Obranou proti tomuto typu hrozeb je vypnutí automatického spouštění obsahu pokud možno pro co nejvíce paměťových médií a pravidelné aktualizace systému.

Příklad

V roce 2019 se mezi uživateli Androidu začal objevovat trojan xHelper, který se v neoficiálních obchodech maskoval jako čisticí aplikace. Po instalaci místo čištění systému okamžitě odeslal svému serveru co nejvíc informací, které sehnal, a naopak do zařízení stáhl sledovací software. Likvidace tohoto trojana byla poměrně náročná, dokázal přežít dokonce i reset do továrního nastavení. Nicméně většina antivirů pro mobilní zařízení se postupně naučila ho zlikvidovat (ale nebylo to jednoduché, uživatel musel „spolupracovat“ (Computer 5/2020).

Trojani se nevyhýbají ani produktům Applu, dokonce mohou být v App Storu potvrzeni jako důvěryhodní. To se stalo například s Trojanem Shlayer, který pod pláštíkem aktualizace Flashe proklouzl právě do App Storu a prošel notifikačním mechanismem (Computer 10/2020).

Trojani se s oblibou maskují také za hry, bankovní aplikace, aplikace pro chytrá zařízení nebo dokonce antiviry. Objevují se také trojani napodobující existující populární aplikace, od kterých se liší třeba drobnou změnou názvu.

Příklad

MSIL/Lockscreen.J je trojský kůň českého původu, který poté, co se dostane do počítače, tento počítač uzamkne (zcela zablokuje), odstaví Správce úloh a zobrazí zprávu, že po odeslání SMS na zadané číslo bude počítač odblokován. Zmíněné číslo je však placené. Jde o tzv. *ransomware*, což je trojský kůň v roli vyděrače (o ransomwaru později v této kapitole). Pokud počítač restartujeme (i bez odeslání SMS), bude odblokován, jen se nedostaneme ke Správci úloh.

Příklad

Trojan Emotet začal svou kariéru v roce 2014 jako bankovní trojan, nicméně postupem let rozšířil své portfolio. Krade nebo šifruje data, dokáže detekovat, že je spuštěn v Sandboxu nebo virtuálním prostředí (tudíž se chvíli chová slušně). Šíří se většinou v e-mailech s napadenou přílohou, a aby zprávy vypadaly co nejreálněji, bývá přílohou často soubor (obvykle wordovský), který byl odcizen na jiném dříve napadeném počítači (Chip 11/2020). Tímto trojanem byly napadeny i jinak poměrně dobře chráněné úřady, například v roce 2020 vládní servery Litvy.

2.1.3 Červ

Červ (worm) se dokáže šířit sám z počítače na počítač většinou pomocí síťových programů či protokolů nebo přes sdílení souborů (využívá bezpečnostní díry v systému a protokolech), je tedy nezávislý na důvěřivosti uživatelů a jejich nutkání spouštět cokoliv, co vypadá zajímavě (na rozdíl od virů a trojanů se nešíří v souborech). Takto zneužít se dají například webové protokoly, e-mailové, IRC, protokoly pro sdílení souborů a další.

Jedinou obranou proti červům je mít aktualizovaný systém a aktualizované bezpečnostní nástroje (antivirus, firewall apod.)

Příklad

Už léta je velmi známý (i mediálně) červ *Conficker*, zejména proto, že infikoval také počítače ozbrojených sil několika států. Také byl nalezen v jedné z německých jaderných elektráren (Computer 6/2016), naštěstí se z uzavřeného systému nemohl spojit se sítí.

Conficker zneužívá bezpečnostní mezeru ve Windows MS08-067. Šíří se přibližně od konce roku 2008, a to přes vyměnitelná paměťová média, síť, sdílené soubory, z důvodu svého zamaskování vypíná automatické aktualizace, Centrum zabezpečení, Defender a zápisy do protokolů ve Windows, dále blokuje přístup na weby zabývající se zabezpečením počítačů. Hlavním úkolem je zapojovat zařízení do botnetu (viz dále).

Účinnou obranou je pravidelné stahování aktualizací a používání aktualizovaného antiviru (to je prevence; po infikování použijeme specializovaný nástroj na odstranění tohoto červa).

Příklad

Velmi obtěžující byl například červ Sasser. Dokázal „odstřelit“ proces `lsass.exe`, přes který jde veškeré přihlašování, kontroly přístupových oprávnění k různým objektům apod., na což Windows reagují restartem. Po restartu se nicméně Sasser vždy znovu aktivoval, opět „odstřelil“ proces `lsass.exe`, systém se restartoval,..., tak dlouho, dokud uživatel neztratil nervy a nevytáhl počítač ze zásuvky.

Z historie (rok 2000) je taky známý červ ILOVEYOU, který se šířil e-maily s podvrženou zprávou „LOVE-LETTER-FOR-YOU.txt.vbs“ (dvojitá přípona, z nichž většina uživatelů viděla jen tu první část, protože ve Windows je naprosto běžné skrývání přípon). Po otevření přílohy bylo náhodně zničeno několik souborů a červ se dále šířil na adresy, které získal ze seznamu kontaktů uživatele.

2.2 Malware podle působení

2.2.1 Spyware

Spyware je program, který z počítače odesílá data bez vědomí uživatele. Do počítače se většinou dostane jako součást jinak užitečné aplikace, mnozí vydavatelé softwaru chápou jako možnost získat představu o rozsahu používání volně (nejen) šiřitelných variant svého produktu. Spyware se také do počítače dostává při prohlížení některých internetových stránek (obvykle s „podezřelým“ obsahem).

Nemusí jít vysloveně o nebezpečný software (vyskytují se možnosti získávání informací pro cílenou reklamu), ale většinou bohužel je (odesílá citlivé informace jako jsou hesla, čísla kreditních karet apod.), může dokonce fungovat jako zadní vrátka do systému (tzv. backdoor). Spyware bývá také používán k přesměrování domovské stránky. Spyware se odstraňuje antispywarovými programy.

Typické projevy spywaru mohou být

- mírné zpomalování počítače,
- změna domovské stránky a problémy s nápravou tohoto problému,
- záhadné chyby při běhu systému a některých procesů, které předtím nenastávaly,
- při používání internetového prohlížeče se často objevují vyskakující (popup) okna,
- připojení na síť je využíváno, i když by zrovna nemělo (to je však neprůkazný argument, některé aplikace si samy stahují automatické aktualizace a jiná data).

Ale pozor, na to nelze spoléhat. Vždy záleží na tom, jak dobře je dotyčný spyware naprogramován. Část výše uvedených projevů se vyskytují spíše tehdy, když programoátor svůj spyware poněkud odflákl nebo když máme slabší počítač, než dotyčný programátor předpokládal.

Existují i speciální typy spywaru, které někdy bývají prezentovány jako samostatná skupina malwaru:

- *adware* obtěžuje uživatele zobrazujícími se reklamami, zejména na malé obrazovce mobilního telefonu to může v horších případech prakticky znemožnit používání zařízení,
- *keylogger* odchytává stisknuté klávesy na klávesnici, obrana pomocí virtuálních klávesnic zobrazených na monitoru byla už bohužel překonána, keyloggery mohou být také hardwarové (malá součástka připojená mezi klávesnici a příslušný konektor na počítači nebo jednoduše drobné nenápadné zařízení v USB portu),
- *hijacker* umí změnit domovskou stránku v internetovém prohlížeči (tj. „unese“ domovskou stránku).

Příklad

V mnoha volně šiřitelných aplikacích pro Windows najdete spyware *OpenCandy*. Některé aplikace nabízejí při své instalaci možnost tento spyware vynechat, jiné o něm jen informují v podmínkách EULA, další se neobtěžují ani tím.

OpenCandy provádí to, k čemu je pro danou konkrétní aplikaci nakonfigurován – může například přidávat do webových prohlížečů lišty, měnit domovskou stránku, ale taky zasahovat do systému či uživatelských nastavení (taky podle toho, jaká oprávnění se mu podaří získat).

Tento spyware odstraníme například pomocí nástroje *AdwCleaner*.

Příklad

Jako spyware se kolikrát chovají i takové aplikace a služby, u kterých by to člověk nečekal. Každou chvíli se objeví nějaká kauza, například v roce 2019 se ukázalo, že mobilní aplikace sítě TikTok zneužívala zranitelnost v systému Android a sbírala MAC adresy uživatelů sítě. Na přímý dotaz přišla odpověď, že teď už to aplikace nedělá (Computer 10/2020).

V roce 2020 přišla další zpráva z oblasti zařízení s Androidem. Webové prohlížeče společnosti Xiaomi (jak ty přímo nainstalované na zařízeních od tohoto výrobce, tak i stažené přes obchod Google Play). Prohlížeče posílaly na weby Xiaomi nejrůznější údaje včetně seznamu navštěvovaných webů, klíčových slov zadávaných do vyhledávání, zobrazovaných zpráv, ale i metadat z daného zařízení. Tomuto špiónovi naprosto nevadilo, že se zrovna surfuje v tzv. „incognito“ módu, i v takovém případě se tato data posílala. Společnost nejdřív reagovala odmítavě (to není pravda...), ale později připustila určité problémy a aktualizací umožnila uživatelům vypnout v incognito módu posílání dotyčných informací, v dalším updatu zpřehlednila možnosti nastavení v prohlížeči, aby bylo jasnější, co se v daných režimech děje. Podrobnější informace můžeme najít na mnoha zpravodajských webech včetně https://www.xda-developers.com/xiaomi-mi-web-browser-pro-mint-collecting-browsing-data-incognito-mode/. O příslušných nastaveních například na https://gadgetstouse.com/blog/2020/05/05/5-ways-to-stop-xiaomi-mi-browser-from-collecting-your-browsing-data/.

2.2.2 Rootkit

Rootkit byl původně pojem ze světa UNIXu, kde znamenal sadu nástrojů použitelných pro získání a udržení oprávnění uživatele root (tak se nazývá hlavní administrátor). Ve Windows je to program, který dokáže skrývat před systémem i antivirovými programy nejen sebe, ale případně i další škodlivý software. Rootkity dokážou skrývat soubory, běžící procesy, klíče registru, služby, síťová spojení, zadní vrátka do systému a další.

Jeho předchůdcem je tzv. *stealth virus*, který se v MS-DOSu napojoval na přerušení související s přístupem na paměťová média a jakýkoliv pokus o své přečtení maskoval falšováním údajů získávaných přes tato přerušení. Rootkity se většinou vyskytují v kombinaci s jiným malwarem.

Běžnými metodami (včetně antivirů) jsou rootkity prakticky nezjistitelné, pro jejich odstranění jsou nutné specializované nástroje (nejznámější jsou zřejmě *Gmer*, *RootkitRevealer* a *AVG AntiRootkit*). Tyto nástroje většinou pracují tak, že k souborům na disku (a jiným potenciálně zmanipulovaným objektům) přistupují dvěma různými cestami – jednou klasickým způsobem přes operační systém, a pak s využitím vlastních knihoven s přístupovými funkcemi. Následně porovnají výstupy obou metod a zjistí případné nesrovnalosti.

Rootkit se do systému dostává často pomocí jiných typů malwaru, proto pro prevenci platí totéž co u trojských koní, virů a dalšího malwaru (pravidelné aktualizace, nepracovat pod účtem s administrátorskými oprávněními, atd.).

Další informace:

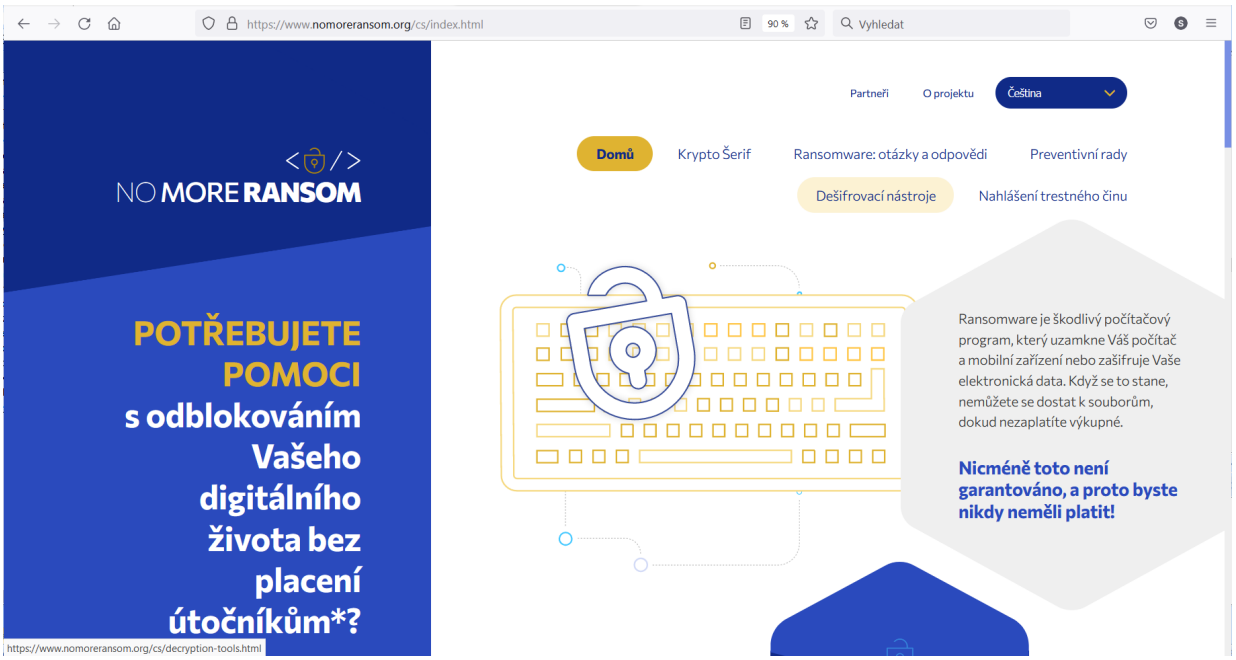
Další informace najdeme na http://www.antirootkit.com.

2.2.3 Ransomware

Ransomware je vyděračský software. Pokud se dostane do systému, buď plně zablokuje počítač nebo zašifruje vybrané soubory, které jsou zjevně pro uživatele důležité (třeba fotografie, videa nebo obecně dokumenty, hry apod.). Následně uživatele informuje, že klíč k odblokování či dešifrování obdrží až po zaplacení určité částky, většinou v bitcoinech (aby byla transakce nevyhledatelná). Typické částky se pohybují v tisících nebo desítkách tisíc korun (podle konkrétního ransomwaru a podle kurzu bitcoinu).

Někdo radši zaplatí, ale některé vyděračské programy se neobtěžují následně zaslat klíč, takže zaplacení nemusí vést k úspěchu.

Zřejmě nejznámějším projektem obrany proti ransomwaru je *No More Ransom* dostupný na webu https://www.nomoreransom.org/. Najdeme zde nejen odpovědi na nejběžnější otázky a další informace, ale také nástroje na dešifrování velkého (a stále se zvětšujícího) množství různých druhů ransomwaru, a navíc je zde nástroj Krypto Šerif pro spolupráci v komunitě při vytváření dešifrovacích nástrojů pro zatím neprolomené druhy ransomwaru.



Obrázek 2.3: Web projektu No More Ransom

Ransomwarem se dnes zabývají prakticky všechny bezpečnostní firmy, často se specializují na konkrétní typy ransomwaru. Obvykle na svých stránkách mají sekci věnovanou této problematice, případně včetně dešifrovacích nástrojů. Proti ransomwaru využívajícímu TeslaCrypt existuje nástroj TeslaDecoder nebo TeslaCrypt Decryption Tool od Cisco Talos.

Nejdřív je třeba vědět, jaký ransomware vlastně naše zařízení napadl. Pokud se sám nepochlubí, nezbývá než porovnávat snímky „informační obrazovky“.

Příklad

Do historie se nepěkně zapsal i červ ransomware Wanna Cry. V roce 2017 se masově rozšířil do celého světa a v některých oblastech doslova zmrazil některá odvětví. Těžce zasažené bylo zdravotnictví v Anglii a Skotsku (zastřešované organizací National Health Service), španělská Telefónica, německé dráhy

Deutsche Bahn, burza FedEx, automobilky Renault a Nissan a státní správa v mnoha zemích.

Tento ransomware zneužíval některé bezpečnostní díry ve Windows včetně využívání exploitů EternalBlue a DoublePulsar. Exploit EternalBlue zneužívá chybu v SMB mechanismu (sdílení souborů a dalších prostředků v lokální síti) a „autoři“ útoku ho předtím odcizili na serverech NSA. Je smutné, že v době útoku už na danou zranitelnost existovala záplata, ale ne každý záplatuje včas...

Příklad

Tragicky nebo alespoň velkými finančními náklady mohou skončit ransomwarové (ale samozřejmě i jiné) útoky na zdravotnická zařízení, zejména nemocnice. Na přelomu let 2019/20 se cílem útoku ruského ransomwaru Ryuk stala nemocnice v Benešově. Nemocnice údajně nezaplatila, přesto se náklady způsobené tímto ransomwarem postupně vyšplhaly na více než 59 milionů korun. Mnoho zdravotnických zákroků totiž zůstalo neproplaceno, protože se záznamy o nich ztratily, mnohé zdravotnické úkony zase nemohly být provedeny v době nefunkčnosti technologií, další část nákladů souvisela s následným zabezpečováním nemocniční sítě, nákupem bezpečnostních systémů a proškolením personálu (Chip 10/2020).

Bohužel jinde šlo i o jiné než finanční náklady. Útok na německou nemocnici v Düsseldorfu měl za následek smrt pacientky (Chip 11/2020). Ransomwaru dnes čelí zdravotnická zařízení po celém světě.

Mezi odbornou i laickou veřejností probíhají diskuse, zda zaplatit či nezaplatit. Ono zřejmě záleží na okolnostech. Sice jsou firmy upomínány, aby zálohovaly a v případě napadení prostě obnovily data ze zálohy, ale je otázka, kterou zálohu pro obnovení vlastně použít. Už jsou totiž pryč doby, kdy ransomware zaútočil hned jak se na zařízení dostal: nejdřív si „obhlédne situaci“, zjistí, co je na zařízení zajímavého, co je tam zranitelného, a nějakou dobu sleduje připojování a odpojování zařízení a větší datové toky na síť, včetně zálohování. Často se stává, že kromě používaných zařízení byly napadeny i zálohy.

Taky je třeba mít na mysli, že pokud zaplatíme, podpoříme tím kriminální živly a potažmo i jejich další působení.

2.2.4 Další typy malwaru

Bloatware, Crapware je software předinstalovaný prodejcem (někdy výrobcem) na zařízení. Může jít o „nevyžádané aplikace“ v trial verzích, ale může jít také o skrytý software, o kterém uživatel vůbec neví.

Příklad

Na noteboocích se množí nebezpečný bloatware. Například na některých noteboocích značky Lenovo bývala předinstalovaná aplikace Lenovo Accelerator Application, jejímž zamýšleným účelem je urychlit spouštění některých programů, ale nezamýšleným důsledkem je zranitelnost dovolující odchytávat komunikaci uživatele, útok Man-in-the-middle (Computer 7/2016). Dokonce samotná společnost Lenovo doporučuje tento software odinstalovat.

Podobný rizikový software bohužel najdeme běžně na noteboocích různých značek – HP, Dell, Asus, Acer a dalších. Vyskytují se případy, kdy tento software často se nacházející na skrytých oddílech disku byl napaden škodlivým softwarem a tím se antiviru poněkud zkomplikovalo léčení stroje.

BackDoor („zadní vrátka“) je malware, který otevírá tzv. zadní vrátka do systému, přes která se dovnitř dostane kdokoliv (počítač pak může být vzdáleně ovládán). Většinou se jedná o zneužití některé bezpečnostní díry v systému.

Zadní vrátka jsou někdy vytvořena úmyslně, například programátor si chce nechat možnost zasahovat do systému i bez informování zákazníka. Tento postup se však může vymstít, protože podobné úseky kódu se dají najít a mohou být zneužity.

Phishing, pharming jsou útoky typické zejména pro uživatele on-line bankovnictví, obecně se jedná o metody používané k podvodnému získáváni citlivých údajů.

Phishing: uživatel je kontaktován (většinou e-mailem) s žádostí o ověření nebo potvrzení informací, případně o uvedení zcela nové verze či podrobném testování existující verze aplikace. V odpovědi pak uživatel má zadat některé citlivé informace, jako například heslo nebo TAN (údajně pro ověření, zda se jedná opravdu o správného uživatele). E-mail je sice podvržený (včetně obsažených odkazů), ale může vypadat reálně.

Navíc bývá uživatel typicky zprávou nějak stresován, například údajným problémem s účtem, rizikem zrušení (čehokoliv, třeba toho účtu), rizikem napadení (některé účty byly napadeny, sdělte nám tyto údaje, abychom si ověřili, zda se to netýká i vás), tvrzením o nelegálních aktivitách uživatele, případně jsou zneužívány známé značky či názvy firem, atd. V ČR jsou notoricky známé phishingové e-maily zdánlivě od České spořitelny. Jedná se o formu sociálního inženýrství.

Pharming: uživatel ve webovém prohlížeči uvede správnou adresu banky, ale (po napadení příslušným malwarem) se ve skutečnosti zobrazí podstrčená stránka. Uživatel nic nepozná, protože stránka vypadá reálně, a „přihlásí se“, čímž své přihlašovací údaje odešle hackerovi. Hacker je pak využije na skutečné stránce banky a účet vybere.

Cryptominer je kód pro nelegální těžbu kryptoměn (nicméně také se tak mohou nazývat naprosto legální programy pro komunitní těžbu kryptoměn). Můžeme se taktéž setkat s pojmem „cryptojacking“.

Využívá výpočetní výkon zařízení (nejen počítače, může jít i o mobil nebo třeba chytrou televizi) k těžbě některé kryptoměny (nemusí nutně jít o bitcoin). Těžba kryptoměn postavených na systému PoW (Proof of Work) je totiž výpočetně velmi náročná a proč si pálit vlastní elektřinu, když hacker může využít zařízení svých obětí?

Může jít o nějakým způsobem skrytý samostatný proces, který se do systému dostal třeba jako trojan, ale také může jít o doplněk do webového prohlížeče nebo dynamický kód stažený z napadené webové stránky, taktéž běžící ve webovém prohlížeči. V posledním případě je reakce nejjednodušší: pokud uzavřeme záložku s takovým běžícím kódem, problém vyřešíme. Ostatní možnosti už tak jednoduché nejsou.

Vzhledem k tomu, že těžba kryptoměn je opravdu velmi náročná (legální těžba probíhá většinou buď na výkonných grafických kartách nebo s využitím speciálních čipů ASIC upravených pro konkrétní kryptoměnu), může se zdát, že z pohledu hackera je neefektivní těžit na málo výkonných procesorech „běžných“ zařízení. Ale co když se takových zařízení spojí třeba stovky, tisíce, desetitisíce,...? Pak už to samozřejmě stojí za to.

Příklad

Bezpečnostní firma Cyble informovala, že na internetu se nachází více verzí hry Super Mario 3 Mario Forever, přičemž některé jsou v pořádku, ale v některých se nachází škodlivý kód. Informace byla v

časopise Chip 09/2023. Za touto hrou nestojí původní tvůrce Maria, tedy společnost Nintendo, vytvořili ji fanoušci. Ovšem dalším „fanouškům“ to naprosto nebrání ve zneužití hry. Z popisu vyplývá, že jde o trojana použitého k těžbě kryptoměn na strojích nic netušících hráčů.

Jak poznat, že jsme napadeni cryptominerem? Obvykle to zjistíme tak, že zařízení je podezřele hodně aktivní, zpomaluje, je navázáno velké množství otevřených spojení s něčím na Internetu.

2.3 Co s tím?

V současné době jsou obvykle různé typy malwaru kombinovány nebo si navzájem „vypomáhají“. Typickou kombinací je malware přibalený do spamu vybavený rootkitem nebo kombinace phishingu nebo sociálního inženýrství a některého jiného typu malwaru.

Na rozdíl od předchozích let, kdy se malware vyskytoval masově (obecný, ve velkém množství), nyní jsou typičtější škodlivé kódy šité tzv. na míru. Častými terči jsou zejména vládní servery a servery firem, hackeři se snaží získat důvěrné informace o státních či výrobních tajemstvích, evidovaných chybách včetně softwarových, zdrojové kódy aplikací, technickou dokumentaci k výrobkům, konfiguraci systémů SCADA (systémy řízení průmyslových procesů), osobní, kontaktní a platební údaje o zákaznících, informace použitelné k vloupání jinam (například v březnu 2011 byl odcizen zdrojový kód pro šifrování tokenů SecurID firmy RSA Security, v květnu byl tento kód použit pro napadení bezpečnostního systému známé americké zbrojovky Lockheed Martin).

Ale pozor, to neznamená, že počítače běžných uživatelů jsou v bezpečí, pro hackery jsou zajímavé jak informace, tak i výkon.

Postup

Jak se bránit?

- Důležitou obranou je pravidelná aktualizace systému (aktualizace síťových nástrojů jsou v ní už zahrnuty), internetového prohlížeče a dalších aplikací – kterýchkoliv, které pracují s nějakými vstupy.
- Používáme antivirus, případně antispyware a firewall, surfujeme v dobře zabezpečeném prohlížeči.
- Vyhýbáme se podezřelým stránkám, neklepeme na všechny odkazy, které se objeví v blízkosti kurzoru myši, chováme se bezpečně. Taky pozor na zkrácené odkazy, u kterých není jisté, ja jakou adresu vlastně vedou.
- Opravdu neklikejte na reklamní bannery!
- Je dobré mít pod kontrolou nastavení automatického spouštění připojovaných médií.
- Nespouštíme programy, kterými si nejsme zcela jisti. Když už něco nového spouštíme, měli bychom si být jisti, co program dělá.
- Pokud to není nutné, nepracujeme pod administrátorským účtem. Pro běžnou práci bychom měli mít účet s omezenými právy a případné administrátorské zásahy řešit možností spustit program jako správce. V současných operačních systémech jsme naštěstí vedeni k tomu pracovat pod běžným uživatelským účtem, nicméně i při občasných chvílích, kdy navyšujeme svá oprávnění, bychom měli být opatrní.

- Pokud často testujeme nové programy, měli bychom to dělat v chráněném prostředí.
- Do webového prohlížeče je možné přidat plug-in, který zablokuje to, co je podezřelé (Flash, JavaScript, Javu, Silverlight, atd.), případně povolit jen na důvěryhodných webech. Pro Firefox existuje NoScript, který je v tomto ohledu bez konkurence. Další zajímavé plug-iny (i pro jiné prohlížeče) jsou Ghostery, BetterPrivacy a další.
- Existují také speciální moduly do prohlížečů odhalující phishing a pharming, obvykle jsou dodávány s antivirovými programy nebo jde o rozšiřující moduly do prohlížečů.
- Před instalací nového programu (ale taky aplikace na mobilním zařízení) si vždy projdeme diskuse, u spywaru tak často najdeme informaci o nebezpečnosti programu. Existují lidé, kteří si naprosto bezelstně například do svého mobilního telefonu nainstalují aplikaci, v jejíž diskusi jsou důrazná varování dříve poškozených uživatelů.
- Některé druhy malwaru (například ransomware Zepto) se šíří v dokumentech. V kancelářských balících bychom proto měli mít vypnutá makra a zapínat je jen u „známých“ souborů.
- Zálohujeme. I když tím problém zcela nevyřešíme (existuje i takový ransomware, který hlídá připojování externích paměťových médií a datové toky a spustí se ve chvíli kdy zálohujeme – napadne počítač i zálohu), může to pomoci.
- Některé bezpečnostní produkty sledují přístupy na disk, a pokud zjistí masivní čtení a zápis dat, okamžitě dupnou na brzdu.
- Do e-mailu (nebo třeba na webovou stránku otevřenou z odkazu v e-mailu) v žádném případě nezadáváme heslo, PIN, TAN, číslo kreditní karty ani jiné citlivé údaje. Pro transport těchto údajů se vždy používají jiné – zabezpečené – cesty. Na Internetu platíme kartou zásadně přes důvěryhodné platební brány.
- Při opouštění bankovních stránek se nezapomínáme odhlásit. Bez odhlášení je teoreticky možné dostat se k účtu přes historii prohlížeče. K zabezpečeným stránkám přistupujeme pouze z důvěryhodného počítače v důvěryhodném umístění, měli bychom si dát pozor například na internetové kavárny.
- Většina malwaru je určena pro Windows, proto je bezpečnější přistupovat k bankovnímu účtu z Linuxu. Linux můžeme spouštět i virtualizovaně bez nutnosti restartu počítače (samozřejmě je nutné, aby měl přístup na síť).
- Pokud máme podezření, že náš bankovní účet či počítač mohl být takto napaden (například se zobrazují podivné chybové zprávy, na přihlašovací stránce se nám něco nezdá), okamžitě kontaktujeme banku a případně necháme tento účet zablokovat (pokud ještě není pozdě).

Poznámka:

V jednom z bodů je zmínka o zkrácených adresách (například adresy začínající bit.ly, ale taky na Facebooku a jiných službách). Pokud chcete vědět, co se za konkrétní zkrácenou adresou doopravdy skrývá, můžete použít službu https://urlex.org/ – stačí zadat zkrácenou adresu a klepnout na tlačítko, objeví se skutečná adresa.

2.4 Spam

Za speciální typ malwaru můžeme také považovat nevyžádanou poštu, spam, třebaže technicky je to spíše distribuční cesta pro malware a samozřejmě obtěžující prvek. Se spamem se setkal snad každý, kdo má a používá e-mailovou schránku.

Postup

Obrana není jednoduchá, ale většinou stačí dodržovat tyto zásady:

- Nikdy neotevíráme e-mail, jehož příjemce neznáme, anebo ho sice známe, ale text v předmětu je podezřelý (není až takový problém zfalšovat adresu). U e-mailu, který otevřeme, si pořádně rozmyslíme, než otevřeme soubor s přílohou (ideální je, když antivirus předem kontroluje maily i jejich přílohy). Pokud to není absolutně nutné, neklepeme na odkazy v e-mailu uvedené. Zákeřné mohou být odkazy typu „Pokud tyto zprávy nechcete dostávat, klikněte . . . “.
- Používáme antispam. Antispamové filtry jsou dnes běžně na mail serverech, ale to nemusí stačit, můžeme mít vlastní antispam (má smysl, pokud poštu stahujeme na lokální počítač).
- Pokud používáme „lehkého“ mail klienta, který je součástí Windows, měli bychom uvažovat o přechodu na něco bezpečnějšího. Z volně šiřitelných alternativ, které jsou mnohem lépe vybavené (nejen co se týče bezpečnosti), je to například Thunderbird.[1]
- Je bezpečnější mít vypnuté zobrazování HTML tagů, nebo alespoň zakážeme automatické načítání externích prvků na stránce (Thunderbird má toto nastavení jako výchozí).
- Nezveřejňujeme svou adresu v „automaticky použitelném“ tvaru. Někdy stačí nahradit zavináč a tečky něčím, co pochopí živý člověk, ale webový robot poněkud obtížněji.
- Pro diskuse a jiné stránky, kde se vyžaduje zadání e-mailu, můžeme mít speciální adresu, kterou používáme jen k tomuto účelu.

Další informace:

Z roku 2021 je tento článek: https://www.cnews.cz/prumerna-ceska-domacnost-denne-celi-temer-10000-hackerskych-utoku-turris/

2.5 Botnet

Botnet je síť botů (web robots, obvykle malwaru) běžících na zmanipulovaných počítačích (zombies) používaných internetovou mafií k různým, ponejvíce nezákonným, účelům. Většina uživatelů předpokládá, že se jich to netýká, ale podle jednoho z otců internetu, Vintona Cerfa, je v současné době až 25 % počítačů[2] součástí některé sítě botů (kdo nepochopil – čtvrtina). Podle odhadů firmy Symantec (známé svými bezpečnostními řešeními, například Norton Internet Security) je *každý den* pro tyto účely infikováno přibližně 50 000 počítačů (údaj z Chipu 6/2009).

[1] https://www.thunderbird.net/cs/

[2] http://gracefulflavor.net/2007/01/27/vint-cerf-25-of-all-pcs-are-part-of-a-botnet/, údaj z roku 2007, dnes je pravděpodobně situace ještě horší co do skutečného počtu.

Obvyklá velikost větších botnetů bývá přibližně půl milionu počítačů. Zřejmě největší objevená síť botů byla vytvořena červem Storm, zahrnuje odhadem 1 milion počítačů.[3]

Sítě botů jsou používány pro aktivity, které jsou nezákonné (bot je jakýsi mezistupeň ztěžující odhalení skutečného pachatele), hromadné (výpočetní kapacita botnetu je mimořádně vysoká) a obvykle výnosné. Jde většinou o rozesílání spamu nebo o DDoS útoky na servery (server je zahlcen požadavky botů, zhroutí se) či těžbu kryptoměn. Bot také dokáže ze zombie odesílat citlivé informace. Botnety jsou výnosné zboží, se kterým se obchoduje na černém trhu.

Počítač může být nakažen více různými způsoby. Bot se dovnitř dostane většinou pomocí spamu, některých červů, trojských koní nebo jiného malwaru. Uživatel většinou ani nepozná, že se něco děje, určitou indikací může být například zpomalení běhu počítače nebo výskyt nevysvětlitelných chybových hlášení.

Na téměř všech zombies běží některá verze Windows, často i pirátská kopie (nelegální, není aktualizován) nebo je operační systém špatně zabezpečený (neaktualizovaný).

Botnety jsou v současné době považovány za velmi vážný problém. Proto se v boji proti nim spojují firmy produkující bezpečnostní software, poskytovatelé internetu a další, a také vznikají speciální týmy soustřeďující se přímo na odhalování a likvidaci botnetů.

Zajímavou zbraní těchto týmů je například *honeypot* („medová vábnička“), který se potenciálnímu útočníkovi jeví jako nechráněný systém (bez bezpečnostních záplat a bezpečnostního softwaru). Takový stroj se s velkou pravděpodobností stane uzlem v síti botů a zde funguje jako obdoba „zadních vrátek“ do botnetu. Odborníci mohou analyzovat malware, který zajišťuje funkčnost botnetu (to pomáhá při vytváření nástrojů k objevení a zničení takového malwaru) a může se jim také podařit dostat se k serveru, přes který jednotlivé boty dostávají instrukce – tzv. CnC (Command and Control, řídicí) server, také sinkhole server, tak se lze dostat k informacím o celé síti aktivních botů.

Příklad

Velmi známý software pro vytváření sítí botů je *Zeus* (také se nazývá ZBot nebo Kneber). Jde o trojského koně (ke koupi na internetu) budujícího rozsáhlé botnety a slídícího po informacích různého charakteru (zejména přihlašovací údaje k sociálním sítím včetně Facebooku, elektronickému bankovnictví, e-mailovým účtům, apod.). Případný zájemce (kupec) má k dispozici software k vytvoření spustitelného souboru bota podle vlastních představ a software k nainstalování na server (sinkhole server). Po vytvoření příslušného spustitelného souboru a instalaci serveru může budovat svou vlastní síť. Skutečný počet strojů nakažených trojanem Zeus není samozřejmě znám, odhaduje se na mnoho miliónů. Hovoří se sice o botnetu Zeus, ve skutečnosti však jde o mnoho dílčích sítí.

Během roku 2010 se v odborném tisku hodně psalo o botnetu *Mariposa*. Opět jde o software pro budování rozsáhlých botnetů (milióny uzlů). Na konci roku 2009 byl sice botnet zničen (španělskou policií), ale podle informací z léta 2010 se Maripose podařilo „vstát z mrtvých“. Velký rozruch způsobilo především odhalení seznamu počítačů, které do botnetu patřily – šlo o mnoho počítačů patřících nejznámějším světovým firmám a Mariposa se dokonce dostala na zařízení HTC Magic (smartphony prodávané Vodaphonem ve Španělsku). Napadené počítače se nacházely v různých částech světa.

[3] http://www.pcworld.com/article/137854/storm_the_largest_botnet_in_the_world.html

Postup

Jak se bránit?

- U dobře zabezpečeného počítače je velmi malá pravděpodobnost napadení botem. Proto bychom měli mít zapnuté automatické aktualizace, instalovaný antivirus, antispyware, firewall, atd.
- Pokud se do internetu připojujeme přes router, zapneme na něm hardwarový firewall. Pozor, také routery mohou být nakaženy botem.
- Používáme zabezpečený internetový prohlížeč, vždy máme zapnuté automatické aktualizace. Pokud vysloveně nepotřebujeme JavaScript, vypneme jeho podporu (zajímavým doplňkem pro Firefox je *NoScript*).
- E-maily necháváme kontrolovat antivirem a používáme antispam.
- U mnohých uživatelů by stálo za úvahu přejít na jiný operační systém.

Obě strany (útočníci i obránci) používají nejnovější technologie. U botnetů jde například o rychlé nalezení náhradního řídicího serveru při odstřižení stávajícího, u obrany jde o aktuálnost a výpočetní výkon při odhalování útočníků (například Panda Cloud Antivirus, Cloud Secure, FireEye MAX Cloud Intelligence Network, atd.).

Další informace:

- Útok vedený z botnetu nemusí nutně znamenat, že síť nebude vůbec fungovat, ale poznat se dá: https://blog.wedos.cz/jak-probihal-zrejme-nejsilnejsi-ddos-utok-v-cesku
- Falliere, N. – Chien, N. *Zeus: King of the Bots*. Článek týmu Symantec Security Response. URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
- *Web společnosti FireEye* (rozcestník k informacím). URL: http://fireeye.com/
- Kratochvíl, P. *Nová hrozba: Botnet Mumba*. Článek v časopise Chip 8/2010, dostupné na: http://www.chip.cz/novinky/bezpecnost/2010/08/nova-hrozba-botnet-mumba
- Kratochvíl, P. *Souboje sítí botů*. Článek v časopise Chip 5/2010, dostupné na: http://www.chip.cz/novinky/bezpecnost/2010/05/souboje-siti-botu

Kapitola 3

Nástroje proti malwaru

Rychlý náhled: Zatímco v předchozí kapitole jsme se zabývali malwarem, v této kapitole se zaměříme na nástroje bojující proti malwaru. Projdeme jak běžné produkty typu antiviru, tak i princip firewallu a postup výběru bezpečnostního produktu.

Klíčová slova: Antispam, antivirus, antispyware, firewall, port, demilitarizovaná zóna

Cíle studia: Po prostudování této kapitoly se budete orientovat v produktech určených pro zabezpečení počítačů.

3.1 Bezpečnostní produkty

3.1.1 Antispam

Detekce spamu je náročný proces, snadno může dojít k omylu. Někdy se stane, že antispam označí jako spam zprávu, která ve skutečnosti není spam.

Antispamy používají většinou tyto techniky:

- *Blacklist* (černá listina) – pokud je adresa odesílatele (resp. IP adresa, ze které je zpráva odeslána) na seznamu, je zpráva pravděpodobně spam.

  Může fungovat také jako *graylist* – taková zpráva je dočasně odmítnuta. Pokud je přesto legitimní, odesílající server se pokusí ji odeslat znovu (při opakovaném obdržení ve stanovené době je už přijata). Spamové servery se s opakovaným odesláním obvykle neobtěžují.
- *Heuristiky* – algoritmus analyzuje předmět a tělo zprávy a hledá typické příznaky spamu (konkrétní slova, typ odkazů apod.).
- *Bayesovské filtry* (statistické, učící se) – je to kombinace heuristických algoritmů a uživatelských zásahů. Uživatel může sám označit zprávu za spam a takto filtr postupně zjišťuje, „učí se“, které prvky jsou pro spam typické. Zpráva je hodnocena – každý „podezřelý“ prvek zvýší pravděpodobnost, že jde o spam (pravděpodobnost se většinou počítá algoritmem navrženým matematikem Bayesem, od toho název metody). Když překročí stanovenou pravděpodobnost, je považována za spam. Tento typ filtru s postupem času zlepšuje svou funkci.

Antispam může být buď rozšiřující modul nějakého mail klienta, anebo samostatný program, který dokáže spolupracovat s prakticky jakýmkoliv klientem (bývá napojen na příslušné přenosové protokoly), na cestě e-mailu je ještě „před“ klientem.

Antispam získáme buď jako součást některého bezpečnostního balíku, nebo zároveň s e-mailovým klientem (například takovýto modul je součástí Thunderbirdu), anebo můžeme instalovat samostatnou aplikaci pro tento účel, například Spamihilator.[1]

3.1.2 Antivirový software

✎ *Antivirový software* slouží především k detekci a odstraňování virů a trojanů, i když v současné době bývá často integrován i s antispywarem, firewallem a dalšími moduly. Obvykle nabízí

- možnost kontroly souborů na disku na vyžádání (on demand) nebo načasovanou,
- rezidentní štít pro kontrolu přístupu,
- e-mailový skener a skener pro stahování z webu,
- modul pro aktualizaci virové databáze a samotného programu,
- další – kontrola ICQ či jiných komunikátorů, léčení napadených souborů, atd.

✎ *Jádro* antivirového programu obvykle obsahuje dvě části – modul pro práci se soubory (identifikace, dekomprimace archivů, emulátor) a modul pro detekci malwaru s implementací těchto metod:

1. *Virové signatury* – pracuje se s virovou databází obsahující signatury známých virů. Tato databáze musí být neustále aktuální, na druhou stranu některé starší viry, které se již neobjevují, bývají z databází postupně vyřazovány. Výhodou je relativní snadnost použití, nevýhodou je statičnost záznamů, mnohé viry a trojské koně tuto metodu dokážou obcházet (nelze použít na dosud neodhalené viry).
2. *Heuristika* – tato metoda dokáže odhalit i některé neznámé viry. Spočívá ve vyhledávání úseků v kódu, které jsou v běžných programech neobvyklé a naopak by se u viru předpokládaly (instrukce pro odstranění souboru bez dotazu, formátování, apod.).
3. *Emulace* – v emulátoru je simulován běh podezřelého programu, v běžných antivirech se tato metoda většinou používá ve zjednodušené formě jako sandbox (píseček).
4. *Detekce chování* (proaktivní ochrana, behaviour blocker) – v rezidentním štítu se neustále monitoruje chování procesů. Pokud se některý proces chová „podezřele“ (pokusy o přístup na internet u aplikace, která to nemá výslovně povoleno, přístup k některým citlivějším souborům, program nemá vlastní okno, pokouší se vytvořit položku v registru pro automatické spouštění po startu systému, atd.), je považován za potenciálně nebezpečný.

✎ Může se stát, že antivir označí za škodlivý nástroj, který je ve skutečnosti neškodný a dokonce užitečný (tomu se říká *false-positive* hlášení, falešný poplach). Tato hlášení jsou důsledkem přísně nastavených heuristik nebo detekce chování. Opakem (taky nechtěným) jsou *true-negative* hlášení, kdy je škodlivý software považován za neškodný.

✂ Nejznámější antiviry:

- Avast! od české společnosti Alwil, pro nekomerční použití zdarma.
- AVG od české společnosti Grisoft, dnes již ovšem patří předchozí jmenované firmě.

[1] http://www.spamihilator.com/

- ClamAV je antivirus často používaný na serverech s nainstalovaným Linuxem, sloužících jako souborový nebo mail server pro stanice s Windows.
- Další – Norton antivirus od společnosti Symantec, NOD32 od slovenské společnosti Eset, Kaspersky antivirus, McAfee, F-Secure, TrustPort, BitDefender, Panda, atd.

Poznámka:

Instalujeme vždy jen jeden antivirus. Kdybychom měli nainstalováno (a spuštěno) více antivirů zároveň, antiviry budou zřejmě jeden druhého považovat za škodlivý software (antivirus totiž provádí mnohé akce jinak typické spíše pro malware, i když pouze z bezpečnostních důvodů) a také může být důsledkem celková nestabilita operačního systému.

Většina velkých firem zabývajících se bezpečnostním softwarem dodává antiviry zároveň s dalším antimalwarem v *bezpečnostních balících*. Jednotlivé moduly těchto balíků dokážou navzájem spolupracovat a také mohou mít část kódu společnou. Proto je toto řešení považováno za optimálnější než instalace různých typů antimalwaru zvlášť, šetří zdroje operačního systému.

Bohužel se vyskytují také *falešné antiviry* (rogue, škodící) – malware, které obvykle metodami sociálního inženýrství přesvědčí uživatele k instalaci (začnou se objevovat hlášení o chybách, spouštět podivné programy, „maže se“ pracovní plocha, apod.). Tento typ malwaru je obzvlášť nebezpečený, protože předstírá, že se jedná o software potřebný k zabezpečení počítače. Proti falešným antivirům se bráníme především pečlivým výběrem bezpečnostního softwaru a metodami naznačenými výše pro malware.

V současné době jsou populární také *on-line antivirové skenery*. Pro jejich provoz se vyžaduje dostatečně rychlé připojení na internet. Samotný antivirus pak není nainstalován na počítači, ale na serveru poskytovatele této služby. Tyto nástroje jsou prakticky neustále v aktualizovaném stavu, další výhodou je, že se nemusejí instalovat (to je důležité – při instalaci antiviru na zavirovaném počítači je pravděpodobné, že chování antiviru bude zmanipulováno).

K nejznámějším on-line antivirům patří například nástroje od firem Eset,[2] Kaspersky[3] a BitDefender.[4] Zajímavý je také VirusScan od Jotti[5] sloužící ke kontrole jednotlivých souborů (zašleme soubor, Jotti jej zkontroluje více různými antiviry).

Nejde jen o to virus objevit, ale také ho odstranit. U většiny malwaru to pro antiviry nebývá problém, někdy však musíme zvolit specializovaný nástroj pro tento účel nebo dokonce pro konkrétní malware. Najdeme je většinou na stránkách výrobců – BitDefender Removal Tools, Avast Virus Cleaner apod.

3.1.3 Antispyware

Antispyware je nástroj proti spywaru, a protože samotný spyware se projevuje jinak než viry, také antispyware pracuje trochu jinak než antivirus. Používá se především metoda „blacklistu“ – černé listiny

[2] http://www.eset.cz/online-skener
[3] http://www.kaspersky.com/virusscanner
[4] http://www.bitdefender.com
[5] http://virusscan.jotti.org

(seznam známého spywaru) a detekce chování. Některé programy tohoto typu se navzájem snesou na jednom počítači.

Dnes tento typ nástroje seženeme nejčastěji jako součást bezpečnostních balíků, ale existují i samostatné antispywarové programy. Z nejznámějších:

- Spyware Doctor je velmi kvalitní komerční antispyware, osekaná verze je zdarma.
- Spybot Search & Destroy je velmi známý volně šiřitelný program (pro nekomerční použití).
- Spyware Terminator je volně šiřitelný i pro nekomerční použití.
- Ad-Aware je pro nekomerční účely zdarma.

Pokud antispyware sice zjistí problém, ale nedokáže ho odstranit, necháme si zjistit potřebné informace a uložit do vhodného protokolu (například Ultimate Process Manager[6] nebo ComboFix[7]), požádat o vyhodnocení protokolu na některé diskusi (např. htttp://viry.cz) a pak pro vyřešení problému použít nástroj, který dokáže zajistit provádění potřebných akcí během načítání jádra systému (dřív než se aktivuje spyware, který chceme odstranit). Pro tento účel se dá použít například The Avenger.[8]

Dříve se pro vygenerování protokolu doporučoval program HijackThis, ten je však nevhodný pro uživatele, který neví naprosto jistě, co dělá. Mnohé ze zpráv, které vygeneruje, jsou ve skutečnosti neškodné objekty.

3.2 Firewall

Firewall je software (nebo taky hardware), který hlídá provoz mezi dvěma sítěmi (obvykle mezi domácí sítí a internetem). Ve firewallu jsou definována *pravidla* pro komunikaci mezi sítěmi, podle kterých reaguje buď povolením komunikace, jejím zakázáním a nebo žádostí o vyjádření uživatele.

Pravidla se obvykle týkají těchto údajů:

- zdroj a cíl komunikace, může být zadán IP adresou,
- číslo portu, přes který se komunikuje (tj. můžeme zablokovat používání některého portu), může jít o zdrojový i cílový port,
- používaný protokol,
- stav spojení, atd.

Firewall může být buď jen *jednosměrný* (filtruje pouze příchozí pakety) nebo *obousměrný* (filtruje příchozí i odchozí pakety). Lepší je samozřejmě obousměrný, dokáže efektivněji zachytit případné vynášení citlivých informací.

Firewall ve Windows XP je pouze jednosměrný. Ve verzi Vista se objevil obousměrný firewall, ale filtrování odchozích paketů je v něm standardně vypnuto (dá se ale zapnout), tedy funguje jako jednosměrný.

Kromě softwarových firewallů existují také *hardwarové firewally* fungující jako mezilehlé prvky sítě. Pokud se jedná o zařízení pro domácnosti nebo malé firmy (SOHO segment – Small Office Home Office), bývají součástí směrovačů (routerů) nebo jiných běžných síťových prvků.

[6] Odkaz a návod k použití najdeme na http://spyware.cz/go.php?p=spyware&t=aplikace&id=47.
[7] Podobně na http://spyware.cz/go.php?p=spyware&t=aplikace&id=54.
[8] Informace včetně postupu na http://spyware.cz/go.php?p=spyware&t=aplikace&id=35.

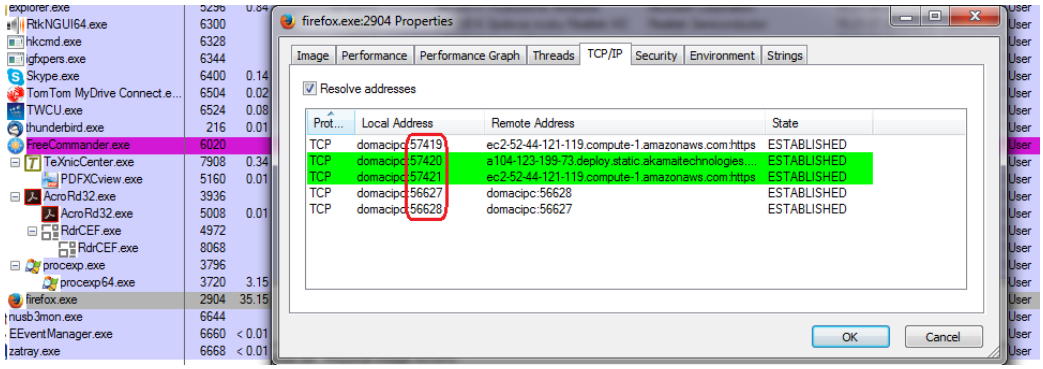
Hardwarový firewall má velkou výhodu v nižším riziku napadení (není závislý na operačním systému klientského počítače). Další výhodou je nezávislost na výkonu počítače – pokud je procesor počítače hodně zatížen, má to vliv i na činnost (především rychlost) softwarového firewallu na tomto počítači nainstalovaného. Hardwarový firewall (třeba vestavěný v jiném síťovém zařízení) takto ovlivněn není.

Z hlediska bezpečnosti je za ideální považována kombinace jednoduchého hardwarového firewallu ve směrovači (to může být třeba ADSL router) a softwarového routeru na počítači, každý z nich jiného typu.

O firewallech by se dalo napsat ještě mnohé (především z pohledu počítačových sítí – různé typy firewallů „vidí“ různé množství informací, podle kterých dokážou filtrovat), ale to bychom se dostali k trochu jinému předmětu.

Nejznámější firewally pro Windows jsou například Comodo Firewall, Sunbelt Personal Firewall (dříve Kerio), ZoneAlarm, Norton Personal Firewall. Firewall bývá také obvyklou součástí bezpečnostních balíků.

Běžný uživatel si většinou s nastavením portů neví rady. Na internetu najdeme stránky se seznamy známých a registrovaných portů používaných různými protokoly.[9] Tyto seznamy jsou však použitelné pro sledování odchozího provozu nebo při nastavování portů na serveru. Ve skutečnosti aplikace mohou používat i jiné porty, než které jsou běžné pro protokoly, se kterými pracují.



Obrázek 3.1: Zjistění portů pro aplikaci v *Process Exploreru*

Porty používané konkrétní aplikací (případně na kterých portech naslouchá) zjistíme například v *Process Exploreru* – v kontextovém menu procesu zvolíme *Properties* (nebo na proces prostě poklepeme) a přejdeme na kartu *TCP/IP* (obrázek 3.1).

Další informace:

Když narazíme na číslo portu, které nám nic neříká, můžeme o něm zjistit potřebné informace na adrese http://www.ports-services.com/.

Úkol

Zjistěte, které porty používají protokoly FTP, WHOIS, SNMP, HTTPS. K čemu se používají porty 22, 25, 110, 10000? Které porty používá Kerberos?

[9] Seznam portů najdeme například na http://www.iana.org/assignments/port-numbers nebo http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. Na české Wikipedii není seznam úplný.

3.3 Podle čeho vybírat bezpečnostní produkt

Existují produkty, které jsou celosvětově známé a používané, a pak produkty, které jsou orientovány na určitou část světa (v tom smyslu, že existuje i takový malware, který je typický pro určitou část světa). Pokud volíme celosvětově známý produkt, pak takový, který má zastoupení i v Evropě. Když se jedná o opravdu známý produkt, obvykle neuděláme chybu.

Další informace:

Mohou se hodit stránky srovnávající výsledky testování bezpečnostních produktů. Najdeme je například zde:

- https://www.av-comparatives.org
- https://www.av-test.org

Protože pro většinu webových služeb je naší bránou do světa webový prohlížeč, existují bezpečnostní testy i pro něj. Informace o testech browserů najdete například na http://www.makeuseof.com/tag/7-browser-security-tests-prevent-exploit-attacks/.

Úkoly

1. Na adresách http://www.av-comparatives.org a https://www.av-test.org zjistěte, jak si momentálně v běžných testech vedou známé antivirové programy.
2. Zjistěte, jak vlastně funguje program *The Avenger*.
3. Vyberte si některý on-line antivirus a zjistěte jeho požadavky na spuštění – operační systém, internetový prohlížeč apod.
4. Na stránce http://www.messagelabs.com/intelligence.aspx otevřete PDF soubor s nejnovější zprávou o stavu bezpečnosti (je tam seznam zpráv od firmy Symantec, zvlášť pro každý měsíc a také několik tématických) a zjistěte, co je nového v oblasti bezpečnosti – jak se vyvíjí četnost jednotlivých typů malwaru apod.
5. Projděte si stránky http://actinet.cz/. Zaměřte se na položku v levém menu *Zpravodajství*.

3.4 Mobilní a další zařízení

Na malých mobilních zařízeních s Androidem není od věci mít taky bezpečnostní software. Vzhledem k tomu, že taková zařízení je jednodušší odcizit, je praktické volit takový, který zároveň pomůže buď dohledat ztracené či odcizené zařízení nebo na dálku alespoň zlikvidovat zneužitelná data.

V obchodě Play najdeme hodně takových aplikací, ale měli bychom mít na paměti, že existují i podstrčené (falešné) bezpečnostní aplikace – je třeba se dívat na recenze (a pokusit se odlišit recenze podstrčené producentem aplikace).

Zařízení od společnosti Apple obvykle nic takového nepotřebují, ale sem tam se vyskytne malware i pro tuto platformu. Nicméně Apple z obchodu odstraňuje bezpečnostní aplikace, protože prý

nejsou zapotřebí. Výhodou je, že zařízení od Applu jsou dobře aktualizovaná (na rozdíl od zařízení s Androidem), takže v těchto systémech existuje méně bezpečnostních mezer.

V současné době by se jen těžko hledala domácnost bez dalších „inteligentních“ prvků s operačním systémem – routery pro přístup na síť, chytré televize, dokonce existují i chytré žárovky. Všechna zařízení by měla mít pokud možno co nejaktuálnější systém a dobře provedenou konfiguraci. Velmi populární jsou „chytré domy“, ale na jejich zabezpečení myslí málokdo.

Hlavním přístupovým prvkem do místní sítě je v domácnostech a malých firmách router (případně ADSL/VDSL modem či podobné zařízení). I tato zařízení se dají aktualizovat (zde jde o upgrade firmwaru), a také je třeba si dát pozor na konfiguraci. Do administrace těchto zařízení se obvykle dostáváme přes webové rozhraní, přičemž zadáváme administrátorské jméno a heslo. Hned po zapnutí bychom se měli přesunout do administrace a změnit administrátorské heslo, protože to přednastavené je obvykle veřejně známé.

Poznámka:

Pozor – pokud resetujete router do továrního nastavení, měli byste zkontrolovat, jestli se neresetovalo i administrátorské heslo.

Wi-fi routery mají ještě jedno heslo – pro běžný provoz. To zadává uživatel, když se připojuje do sítě. V administraci bychom měli nastavit vhodnou úroveň zabezpečení (dnes typicky WPA2), a „provozní“ heslo by mělo být dostatečně silné. Pokud toto zanedbáme, může být důsledkem v lepším případě to, že soused využívá naši síť, v horším případě může být přístup do naší sítě zneužit pro nelegální činnost. A odpovědnými bychom byli my.

Další informace:

Na adrese http://www.routerpasswords.com/ je seznam přednastavených přihlašovacích údajů pro různé routery.

Poznámka:

Čím dál chytřejší jsou taky naše auta. U některých modelů byly bezpečnostními experty předvedeny útoky na řídicí systém, přičemž se hacker dostal dokonce i k ovládání brzd, bezklíčovému vstupu, atd. Často je problém v tom, že automobil dokáže se svým okolím komunikovat bezdrátově (přes Wi-fi, Bluetooth a další technologie), ale bezpečnostně kritické systémy nejsou plně odděleny od zábavních a pomocných systémů.

Kapitola 4

Projekty a licence

Rychlý náhled: Posledním „multiplatformním“ tématem jsou licence. Tato kapitola uvádí do problematiky (především softwarových) licencí a uvádí vlastnosti nejpoužívanějších licencí pro software a dokumenty.

Klíčová slova: Licence, open-source licence, proprietární licence, OSI, freeware, free software, Public Domain, copyright, copyleft, GNU, EULA, GNU GPL, GNU LGPL, BSD, FDDL, GNU FDL, Creative Commons, kompatibilita licencí, duální licencování

Cíle studia: Po prostudování této kapitoly získáte přehled o nejpoužívanějších licencích pro software a dokumenty.

4.1 Základní pojmy

Nehmotné produkty jako software nebo dokumenty bývají distribuovány pod určitou licencí. Většina licencí ve světě softwaru je vpodstatě dvojího druhu: *proprietární* (uzavřené) a *open-source* (svobodné, s otevřeným zdrojovým kódem). V proprietární licenci autor jako součást licenčního ujednání přesně vymezuje způsob využití licencovaného díla (u softwaru například za jakých okolností může/nemůže být produkt používán, třeba „pro nekomerční použití zdarma, pro komerční použití nutno zakoupit...“, na kolik zařízení maximálně může být nainstalován, atd., obvykle nemáme k dispozici zdrojový kód programu. Svobodná licence uživatele tolik neomezuje (obvykle se nerozlišuje způsob použití, počet počítačů, apod.), a máme k dispozici zdrojový kód, který si můžeme přizpůsobit „k obrazu svému“.

Poznámka:

Pozor na spojovník: píšeme „open-source licence“ (se spojovníkem), pokud se jedná o přídavné jméno, resp. přívlastek, kdežto „Open Source je trend...“ (s mezerou místo spojovníku), pokud to je podmět či předmět ve větě. Formulace „licence je typu open-source“ je podobný případ jako ten první.

Nic z toho neurčuje, zda za produkt platíme nebo ne. U obou druhů můžeme narazit na komerční a nekomerční variantu.

Proprietární licence omezuje možnosti využití distribuovaného produktu. Naproti tomu open-source licence říkají, že když už produkt některým legálním způsobem získáme (není stanoveno jak), pak ho můžeme svobodně používat (včetně modifikace – pozměníme zdrojový kód a přeložíme ho).

To, že je produkt distribuován pod open-source (tedy svobodnou) licencí, ještě neznamená, že s ním můžeme dělat opravdu cokoliv. V licenčních ujednáních například bývá klauzule o tom, že pokud produkt pozměníme a dále distribuujeme, nemůžeme ho vydávat za své dílo, ale musíme uvést původního autora. Jinou typickou klauzulí může být požadavek, že při následném distribuování nemůže být použita jiná než původní licence.

Zatímco Windows jsou poskytovány pouze pod proprietární komerční licencí EULA a případně jejími variantami typu hromadné licence, zvýhodněné licence pro školství nebo OEM, ve světě systémů UNIXového typu je používána řada různých licencí. Většina UNIXových systémů je distribuována pod komerční nebo nekomerční open-source licencí.

✎ Definici Open Source vytvořila a tento projekt udržuje nezisková organizace *Open Source Initiative* (OSI).[1] Pokud někdo chce vytvořit a používat další licenci typu open-source (tím není myšlen nový produkt pod existující licencí, ale opravdu novou licenci), musí požádat OSI o certifikaci této licence jako Open Source. Když OSI zjistí, že licence odpovídá definici Open Source, je certifikace udělena. Pro open-source software se také používá také pojem *svobodný software* (free software).

✎ Freeware a free software není totéž. *Freeware* je volně (zdarma) dostupný software, ale neříká to nic o licenci, pod kterou je distribuován (může být proprierální, free v tomto případě znamená „zdarma“).

Free software (distribuovaný často pod licencí GPL) je odvozen od jiného významu slova free – svobodný (můžeme si s ním dělat víceméně co chceme, když už se k němu dostaneme). Bývá většinou volně dostupný (volně ke stažení na internetu), ale nemusí (pak je za peníze, tedy komerční). Takže oba pojmy se částečně překrývají, co se týče příslušných produktů (existují produkty, které jsou obojí), ale ani zdaleka to nejsou synonyma.

✎ Vedle proprietárních a open-source licencí existují také licence typu *Public Domain* (česky také „volné dílo“). Tento typ licencí je naprosto svobodný, uživatelé si s takto šířeným softwarem mohou dělat opravdu co chtějí včetně nejrůznějších úprav a distribuce pod jiným typem licence. Jako Public Domain se také označují díla, u nichž vypršelo majetkové autorské právo (například tehdy, když uplynulo více než 70 let od smrti autora), případně se autor svých práv vzdal. Ovšem ani u produktu s licencí Public Domain se nikdo jiný nesmí prohlašovat za autora.

✎ Licence můžeme dělit na copyrighty a copylefty. *Copyright* obvykle znamená, že to, co je licencováno, můžeme jistým způsobem používat, ale nesmíme do toho zasahovat a nesmíme to dále bez dovolení distribuovat (pouze autor má právo rozhodovat o „kopírování“, tedy má výhradní právo – right – na vytváření kopií – copy).

Copyleft umožňuje nejen používání, ale i možnost úprav (třeba zdrojového kódu) i další distribuci (vytváření a distribuování kopií není radikálně omezeno). Možnost úprav bývá ale omezena s tím, že při dalším distribuování musí být zaznamenáno, o jaké úpravy šlo, kdo je provedl a kdo je původní autor. Hlavním principem copyleftu je nutnost poskytnout uživateli stejná práva k produktu, jaká má distributor či producent (který je také často uživatelem vzhledem k jinému distributorovi a producentovi).

✎ *GNU*[2] je projekt, v rámci kterého je vytvářen svobodný software na profesionální úrovni. Samotná

[1] http://opensource.org/
[2] http://www.gnu.org/

zkratka je rekurzivní: GNU's Not UNIX, vznikla pravděpodobně ve snaze odlišit licencování od komerčních UNIXů (tehdy už/ještě nebyly volně šiřitelné UNIXy jako je například OpenBSD).

Poznámka:

GNU není licence, ale projekt.

Do projektu se může zapojit kdokoliv, kdo chce svými programy přispívat do už velmi rozsáhlé množiny volně šiřitelných, ale přesto velmi kvalitních programů, dále každý uživatel, který dobrovolně testuje beta verze těchto programů a o případných chybách informuje programátora. Rozsáhlost projektu mnohé překvapuje právě proto, že v mnoha případech jde vlastně o práci zdarma.

4.2 Nejpoužívanější licence

4.2.1 Licence určené pro software

EULA (End-User Licence Agreement – dohoda s koncovým uživatelem) je proprietární licence typu copyright používaná společností Microsoft a také dalšími společnostmi produkujícími software především pro operační systém Windows. Tato licence omezuje uživatele softwaru v oblasti úprav (software může být používán pouze „obvyklým způsobem"), počtu používaných kopií (zvláště v případě OEM softwaru je licence omezena jen na konkrétní počítač, při instalaci na jiný porušujeme podmínky licence) a také možností distribuce (distribuce uživatelem je obvykle považována za pirátství, nezákonné šíření).

Poznámka:

Na rozdíl od dále uvedené GPL má autor softwaru distribuovaného pod licencí EULA možnost licenční podmínky dále upravovat (obvykle zpřísňovat). Proto je doporučeno text licence důkladně pročíst ještě před instalaci takového programu, aby uživatel nebyl překvapen důsledky odsouhlasení podmínek licence.

Kromě toho, že EULA silně omezuje možnosti využití softwaru pod ní distribuovaného, obsahuje také klauzuli o tom, že autor neodpovídá za škody vzniklé provozováním softwaru. Tato klauzule je obecně hodně obvyklá u různých licencí, i když z právního hlediska je napadnutelná ve většině států světa.

Obhajobou podmínek licence EULA je známa především organizace BSA (Business Software Alliance). Jde o mezinárodní nevládní sdružení producentů softwaru (z velké části financované Microsoftem), které v České republice nemá oficiální zastoupení (ani právní subjektivitu) a také samozřejmě nemá pravomoci policie.

GNU GPL[3] je rekurzivní zkratka z GNU General Public License), tuto licenci vytvořil Richard Stallman pro projekt GNU. Patří mezi copylefty a jedná se o open-source licenci. Hlavní vlastnosti:

- Software šířený pod touto licencí je volně poskytován včetně zdrojového kódu. Znamená to, že distributor, který pod touto licencí poskytuje binární (přeložený) software, musí poskytnout také

[3] Na http://www.gnu.cz/article/32/ je neoficiální překlad do češtiny, oficiální znění nejnovější verze je na http://www.gnu.org/licenses/gpl.html.

zdrojové kódy a všechny další potřebné soubory (například makefile popisující způsob překladu), a to buď stejným způsobem jako ty binární, anebo jiným akceptovaným.

- Je dovoleno provádět změny v kódu a dále software šířit i po těchto změnách, ale vždy musí být uvedeno jméno původního autora (GPL rozhodně nepopírá autorská práva), upozornění, že program byl změněn a datum této změny. Součástí distribuovaného produktu musí být i znění licence.
- Pokud byl software pozměněn, musí se původce změny o tuto změnu „podělit“ a vhodným způsobem zveřejnit (může to být i prostřednictvím původního autora). Vylepšení nesmí být „sysleno“, autor změny se o tuto změnu musí podělit s ostatními.
- Pokud je software šířený pod GPL dále distribuován, musí to být opět pod licencí GPL (i v případě, že tento software byl pozměněn).

  Při zásazích toto ustanovení platí i v případě, že by z původního programu zůstal třeba jen „poslední řádek kódu“ – reálně to také znamená, že když je knihovna distribuována pod GPL, nelze ji nalinkovat do programu šířeného pod jinou licencí (ani zároveň s ním distribuovat). Proto GPL nebývá pro knihovny většinou používána, k tomu účelu slouží LGPL.
- Pokud je software šířen pod licencí GPL, nesmí autor (ani distributor) přidávat žádné další podmínky omezující využívání tohoto softwaru (tato podmínka je výše zmíněna jako *copyleft*).
- Software poskytovaný pod GPL je bez záruky v rámci právního systému určitého státu. Je to klauzule podobná té, která byla uvedena u EULA.
- Cokoliv je distribuováno pod GNU GPL, musí ve vhodné formě obsahovat plné znění této licence (například u softwaru může být v textovém souboru distribuovaném zároveň se softwarem).

GNU GPL neznamená software zdarma, i když tomu tak často je. Distributor může za produkt požadovat peníze, i když sám ho získal zdarma (to je případ „krabicových verzí“ Linuxu, nazýváme je komerční distribuce). Platí se za zkompletování, přidané nástroje, příručky, poskytovanou podporu (aktualizace systému přes internet, pomoc při instalaci nebo nenadálých problémech, ...) a případné výhody (např. členství v klubu).

Asi nejznámější software distribuovaný pod GNU GPL je jádro operačního systému Linux, dále je spolu s LGPL běžně používaná pro software patřící do projektu GNU.

✎ **GNU LGPL**[4] znamená GNU Lesser GPL. Je to licence odvozená z GPL. Rozdíl oproti GNU *General* Public License je v tom, že knihovny (obecně kód) zveřejněné pod LGPL mohou být používány i v programech pod jinou licencí včetně licencí proprietárních, tedy může být v jednom výsledném produktu kombinována s jinými licencemi ostatních částí produktu.

✎ **BSD** (Berkeley Software Distribution) je licence, pod kterou je dnes distribuováno hodně systémů UNIXové větve BSD, například OpenBSD.

Ve své základní podobě umožňuje volnou distribuci a také volné využití části zdrojového kódu, včetně používání tohoto kódu v systémech pod uzavřenou (closed, komerční) licencí jako je Solaris nebo MacOS X (ale ne naopak, v softwaru distribuovaném pod BSD nesmí být použit uzavřený kód). Je považována za mnohem volnější než GPL.

Na rozdíl od GNU GPL je BSD licence typu copyright. Projevuje se to především v nutnosti uvádět některé povinné údaje včetně jmen autorů, a také v možnosti distribuovat produkt pod jinou,

[4] Nejnovější verze je na http://www.gnu.org/licenses/lgpl.html.

více omezenou licencí (například – když programátor použije část kódu původně distribuovanou pod BSD, není vázán nutností použít BSD i pro svůj výtvor).

BSD licence, stejně jako LGPL a některé další licence, je *kompatibilní* s GPL (týká se to BSD v tzv. revidované formě – „tříbodové“), proto je možné kód původně licencovaný BSD sloučit s kódem licencovaným GPL. Ovšem díky klauzulím v GPL je nutné takto sloučený software šířit pod licencí GPL.

CDDL (Common Development and Distribution License) je open-source licence, kterou vytvořila společnost Sun Microsystems, aby pod ní uvolnila svou variantu UNIXu Solaris pod názvem OpenSolaris. Jsou pod ní distribuovány i některé další produkty společnosti Sun, například souborový systém ZFS. Tato licence je typu open-source, ale *nekompatibilní* s GPL, proto kód z OpenSolaris a jiných takto distribuovaných projektů se nesmí použít v softwaru distribuovaném pod licencí GPL.

4.2.2 Licence určené pro dokumenty

Také dokumenty (dokumentace softwaru, ale také webové stránky, knihy apod.) bývají distribuovány pod určitými licencemi.

GNU FDL (GNU Free Documentation License) je licence určená především pro dokumentaci k programům vytvářeným v projektu GNU. Je poměrně hodně podobná licenci GPL, ale přizpůsobená požadavkům kladeným na dokumentové licence.

U děl šířených pod FDL musí být uvedeni všichni současní i předchozí autoři díla a veškeré změny, které postupně byly na díle provedeny. Pokud je dílo dále distribuováno, pak opět pod FDL bez jakýchkoliv změn podmínek licence. Distribuci a používání díla takto šířeného nelze nijak omezovat, ať už přidanými podmínkami nebo technickými prostředky (DRM).

Podobně jako u GPL, i zde je nutné distribuovat dílo včetně znění licence. To sice není na překážku u programů, ale u dokumentů ano – pokud dokument nebo jeho část vytiskneme, měli bychom správně vytisknout i text licence a přiložit ho. To je jeden z důvodů, proč Wikipedia přešla od licence FDL k CC-by-sa (viz dále). Obdobná databáze Navajo zůstává u FDL.

Je zajímavé (ale smutné), že GPL a FDL jsou navzájem nekompatibilní.

CC[5] (Creative Commons) je projekt zahrnující více různých svobodných licencí určených především pro zveřejňování autorských děl na internetu (není vhodná pro software ani pro dokumentaci k němu). Součástí projektu je taky souhrn metadat použitelných na dílo a jeho licenci, která mají usnadnit automatické zpracovávání (především vyhledávání) podle různých kritérií.

CC licence jsou kombinací některých z těchto vlastností (licenci si lze poskládat použitím/nepoužitím jednotlivých vlastností):

1. Attribution (*by*) – ať se s dílem děje cokoliv, vždy musí být uveden autor.
2. Noncommercial (*nc*) – nekomerční, určené pro nevýdělečné účely.
3. No derivate works (*nd*) – pokud je dílo pozměněno, nesmí být distribuováno (tj. když distribuovat, tak jen v původním znění).
4. Share alike (*sa*) – pokud je dílo dále distribuováno, pak jen bez změny licence.

Obvykle se předpokládá použití první vlastnosti (*by*), ostatní lze libovolně přidávat. Vlastnosti *nd* a *sa* se navzájem vylučují, nelze je kombinovat v jedné licenci. Výsledné licence se pak označují podle

[5] http://creativecommons.org/

kombinace vlastností, které zahrnují, například CC-*by-sa* zahrnuje první a poslední uvedenou vlastnost (musí být uveden autor a dílo má být dále distribuováno vždy jen pod licencí CC-*by-sa*).

Možné kombinace najdeme na http://creativecommons.org/licenses/, kdokoliv si může volně zvolit některou z těchto možností a použít pro šíření svého díla.

K nejznámějším projektům licencovaným pod licencemi CC patří Wikipedia a Flicker.

4.2.3 Kombinování licencí

V předchozím textu byla zmíněna možnost kombinování více licencí tím způsobem, že knihovnu distribuovanou pod jednou licencí připojíme k programu distribuovanému pod jinou licencí, případně v projektu použijeme více knihoven, z nichž každá má jinou licenci. Tomu říkáme *skládání licencí* a je možné jen tehdy, když jsou skládané licence navzájem kompatibilní (například GNU LGPL je možné takto používat, kdežto původní GNU GPL ne).

Některé licence jsou takto kompatibilní jen jednosměrně (pokud je pod touto licencí distribuován výsledný produkt, můžeme v projektu používat knihovny s jinými licencemi, ale pokud je pod takovou licencí distribuována knihovna, nemůže mít výsledný produkt jinou licenci).

Kompatibilita může být omezena jen na určitý způsob použití. Například může být dovoleno používat v projektu dvě knihovny s různými licencemi, ale nemusí být dovoleno spojit tyto dvě knihovny do jediné.

Nekompatibilní licence se dají kombinovat pouze při *duálním* (nebo obecně vícenásobném) licencování – jeden produkt (jako celek) je poskytován pod více různými licencemi zároveň. Typickým příkladem je kombinace nekompatibilních licencí FDL a GPL pro příklady kódu v projektu GNU, aby bylo možné ukázky kódu vkládat jak do dokumentace, tak i do samotných programů.

Příklad

Některé produkty mají své licencování vyřešeno poněkud složitě. Typickým příkladem je Mozilla Firefox, jehož zdrojové kódy jsou šířeny pod třemi licencemi zároveň (triple-licensing) – MPL/GPL/LGPL, kde MPL[6] je Mozilla Public License. Samotný (přeložený) program je pak šířen pod licencí EULA. Díky trojitému licencování zdrojového kódu je možné tento kód přeložit (s případnými úpravami) a dále distribuovat, ale již pod jiným názvem a s jiným logem.

Úkoly

1. Zjistěte, jaký je vztah mezi projektem GNU a Linuxem.
2. Najděte informaci o *GNU Hurd* – co to je?
3. Podívejte se, které licence s GNU souvisejí a jakou roli v této problematice hraje organizace FSF (Free Software Foundation) – http://www.fsf.org/.
4. Zjistěte, zda je GNU GPL verze 3 kompatibilní s GNU GPL verze 2 (informaci najdete v seznamu licencí na http://www.gnu.org/licenses/license-list.html).

[6] http://www.mozilla.org/MPL/MPL-1.1.html