Zase ty viry ...

Kamil Malinka, Radim Peša, ÚVT MU

S fenoménem počítačového viru se setkáváme už více než dvacet let. Mohlo by se zdát, že je to více než dostatečná doba na nalezení ochrany proti šíření počítačových virů a obecně škodlivého kódu. Opak je však pravdou. S počítačovými viry se setkáváme stále; a co hůř – jejich hrozba není rozhodně menší než dříve.

Princip počítačového viru je stále stejný. Je to počítačový program, který se dokáže šířit bez vědomí uživatele. Postupem doby se měnil způsob šíření v závislosti na technologií používaných k přenosu informací. Po pionýrských začátcích s přenosem na disketách, přibylo později šíření elektronickou poštou, počítačovou sítí, stažením z www stránek či přenosem na USB médiích. Velmi podstatně se ale změnil důvod, proč jsou viry vyvíjeny a šířeny. Z původní zábavy asociálních individuí se vyvinulo odvětví kriminální činnosti, které generuje svým autorům finanční příjem. O to více je potřeba si dávat pozor, protože cílem velké části šířeného škodlivého kódu je generování zisku na úkor poškozených uživatelů ve formě krádeže osobních údajů, dat nebo přímo peněz z kreditních karet a účtů. V některých případech se váš infikovaný stroj může stát tzv. *zombie strojem*. Takto se v bezpečnostním žargonu nazývá zařízení, které slouží nejen legitimnímu majiteli, ale také útočníkovi, který nad ním bez vědomí oprávněného majitele převzal správu. Přes tyto stroje mohou následně přicházet další útoky.

Aby se znovu neopakovalo již mnohokrát napsané, připomeňme si pouze některé nové hrozby, které se objevily v posledních měsících, a na které bychom si měli dávat pozor.

1 Útoky z www stránek

Novým nebezpečím je možnost útoku škodlivého kódu při prohlížení www stránek. V předchozích letech se tato hrozba týkala především webových serverů poskytujících nelegální software (warez) nebo pornografický obsah. Návštěvníci ostatních „normálních" webových serverů se mohli cítit relativně v bezpečí. Situace se však radikálně změnila. Podle [1] jsou v současné době útoky z www stránek (web-based attacks) nejčastějším způsobem šíření škodlivého kódu. Typický útok z www stránek má následující průběh:

1. Útočník vyhledává jakékoli (ideálně hojně navštěvované) webové servery a pokouší se do jejich obsahu implantovat škodlivý kód nebo skrytý odkaz, který na škodlivý kód hostovaný na jiném www serveru odkazuje. K vložení škodlivého kódu útočník zneužívá existující chyby webového serveru nebo chyby, které jsou obsaženy v kódu hostovaných www stránek.
2. Škodlivý kód umístěný na www server se při přístupu uživatele na webové stránky příslušného serveru stáhne do prohlížeče na počítači uživatele.
3. Škodlivý kód se v počítači uživatele aktivuje a provede naplánované akce – sběr uživatelských hesel, šíření na další počítače v síti, instalace trojského koně a čekání na další příkazy.

Pro přístup z webového prohlížeče do operačního systému může škodlivý kód využít neopravené chyby webového prohlížeče, které mu umožní získat potřebný přístup k systému. Mimo chyb v prohlížečích webových stránek jsou často zneužívány i chyby v modulech třetích stran, přehrávačích multimédií nebo prohlížečích dokumentů.

Další využívanou možností jak zajistit spuštění škodlivého kódu s potřebným oprávněním, je oklamání uživatele. Může se jednat například o oznámení, že je potřeba nainstalovat novou (velmi užitečnou) softwarovou komponentu. Pokud uživatel zprávu potvrdí a dá souhlas k instalaci, software se nainstaluje a spustí.

2 USB viry

Novým způsobem šíření počítačových virů jsou USB paměťová média. Vypadá to trochu jako návrat do pionýrských začátků, jen diskety jsou nahrazeny USB pamětmi.

USB viry pro své šíření využívají vlastnost automatického otevření média díky úpravě souboru `autorun.inf`, který řídí automatické spuštění

po vložení USB disku do počítače. Systém Windows ve standardním nastavení automaticky vykoná příkazy popsané v tomto souboru. Tedy ke spuštění viru může dojít už při samotném vložení USB paměti do počítače! Automatické spouštění se týká i jiných médií, jako jsou například CD a DVD disky.

Doporučujeme proto dodržovat následující zásady:

1. Používejte aktualizovaný antivirový program.
2. Nepoužívejte administrátorská oprávnění při běžné práci.
3. Vypněte automatické přehrávání výměnných médií. Postup je uveden např. v dokumentu [2]. Jedná se o účinný způsob zamezení šíření USB virů, protože se tím zamezí automatické aktivaci škodlivého kódu při vložení média určeného pro automatické spuštění.
4. Dodržujte hygienu práce s USB médii: nevkládejte do svého počítače zbytečně cizí USB paměti a naopak nepoužívejte své USB paměti u počítačů, kterým nedůvěřujete.
5. Pokud není možné počítač pravidelně aktualizovat (například z důvodů provozu specializovaného softwaru vázaného na specifickou verzi OS), izolujte počítač sítově od nezabezpečené části počítačové sítě a internetu.
6. Aktualizujte i přídavné komponenty webových prohlížečů a aplikační software.
7. Používejte personální i síťový firewall pro omezení síťových protokolů a adres, které nevyužíváte.

Literatura

[1] Symantec Global Internet Security Threat Report, Trends for 2008, `http://www.symantec.com/business/theme.jsp?themeid=threatreport`

[2] K. Malinka. USB viry na vzestupu. `http://ics.muni.cz/~malinka/usbviry.pdf` □