KAPITOLA 4

Klasifikace metod infekce

„Veškeré umění je imitací přírody."

– Seneca

V této kapitole se dozvíte o běžných technikách infekce počítačových virů, které se zaměřují na různé formáty souborů a systémové oblasti.

4.1 Boot viry

První známé úspěšné počítačové viry napadaly tzv. boot sektory disků. V roce 1986 vytvořili na IBM PC dva pakistánští bratři první takový virus pojmenovaný jako Brain.

V dnešní době se technika infekce boot sektoru téměř nepoužívá. S bootovacími viry byste se nicméně měli seznámit, protože dovedou infikovat počítače bez ohledu na operační systém, který je na nich nainstalovaný.

Boot viry zneužívají procesu startování osobních počítačů typu PC. Protože většina počítačů neobsahuje operační systém v paměti ROM (Read-Only Memory, paměť pouze pro čtení), potřebují nahrát systém odněkud odjinud – například z disku nebo z lokální počítačové sítě.

Typický disk IBM PC je organizován do čtyř oblastí (tzv. partitions), které mají na některých operačních systémech, jako je třeba MS-DOS a Windows NT, přiřazená jednotlivá písmena abecedy, většinou C:, D: atd. Písmena disků jsou specifikem jednotlivých operačních systémů – například UNIXové systémy místo nich používají tzv. přípojné body (mount points). Většina počítačů používá pouze dvě oblasti, které jsou být uživatelům zpřístupněny. Někteří dodavatelé počítačů, jako například COMPAQ a IBM, často používají skryté diskové oblasti k uložení dodatečných nástrojů BIOSu. Skryté oblasti nemají přiřazeno žádné písmeno abecedy, čímž je přístup k nim více ztížen. Dobré nástroje, jako třeba Norton Disk Editor, ale umí takové oblasti na disku odhalit (diskové nástroje používejte velmi opatrně – můžete si s nimi nechtěně poškodit vaše data!).

Počítače typu PC obvykle načítají OS z pevného disku. U dřívějších systémů ovšem nebylo pořadí zavádění definováno, a proto se počítač pokusil vždy bootovat z disketové mechaniky, což vytvářelo vhodné prostředí pro aktivaci počítačových virů ještě před startem samotného operačního systému. ROM-BIOS tedy přečte první sektor zaváděcích disků dle jejich pořadí specifikovaného v BIOSu a v případě úspěchu jej uloží do paměti na adresu 0:0x7C00 a spustí[1].

Na novějších systémech je každá disková oblast rozdělena na další oblasti. Disk se vždy adresuje přes hlavu, stopu a sektor. Master Boot Record (MBR) je vždy umístěn na hlavě 0, stopě 0, sektoru 1, což je první sektor na pevném disku. MBR obsahuje generický kód určený pro konkrétní procesor, který vybere aktivní bootovací oblast z tabulky rozdělení disku (tzv. partition table, PT), která se nachází v datové oblasti MBR. Na začátku MBR je krátký kód, kterému se říká zavaděč (boot strap loader).

Každá položka v PT obsahuje:

- Adresu prvního a posledního sektoru oblasti.
- Příznak, zda-li je oblast bootovatelná.
- Typ oblasti.
- Offset prvního sektoru oblasti od začátku disku v sektorech.
- Velikost oblasti v sektorech.

Zavaděč najde aktivní oblast a nahraje její první logický sektor jako boot sektor, který obsahuje kód specifický pro konkrétní operační systém, narozdíl od MBR, který je určen pro obecné použití nezávisle na OS. Takto IBM PC jednoduše podporují více oblastí s různými souborovými a operačními systémy, nicméně tím rovněž usnadňují práci počítačovým virům. Kód z MBR je možné jednoduše nahradit virovým kódem, který použije originální MBR poté, co nahraje sám sebe a dále zůstává v paměti (v závislosti na nainstalovaném operačním systému). V případě MS-DOSu mohou boot viry zůstat v paměti a infikovat za běhu další média. Pár šikovných boot virů, jako například Exebug, vždy donutí počítač, aby je nahrál do paměti a pak dokončí bootovací proces. Exebug mění nastavení BIOSu v paměti CMOS takovým způsobem, aby zmátl počítač a on předpokládal, že systém neobsahuje žádnou disketovou mechaniku – počítač tedy prvně nabootuje z MBR a jakmile je virus aktivován, zjistí, zdali je disku A: disketa. Pokud ano, pak nahraje boot sektor z diskety a předá mu řízení. Pokud se pokusíte nabootovat z diskety, virus se vás pokusí oklamat, abyste si mysleli, že jste z ní skutečně nabootovali, ačkoliv se tak nestalo.

V případě disket je boot sektor prvním sektorem, ve kterém je uvedeno, jaké soubory operačního systému se mají nahrát, jako například IBMBIO.COM a IBMDOS.COM.

Proto se doporučuje nastavit proces bootování tak, aby se prvně bootovalo z pevného disku. V prvních generacích IBM PC nebyl takto bootovací proces navržen, takže pokud byla disketa v jednotce A:, počítač se pokusil nabootovat z ní. Boot viry využívají právě tuto chybu v návrhu, která se dá omezit správným nastavením bootovacího procesu.

> **Poznámka**
>
> Pokud máte v počítači připojený SCSI disk, systém nemusí být schopen z něj nabootovat, protože k těmto diskům není možné přistupovat přímo z BIOSu.

Následující části podrobně rozebírají druhy technik infekce MBR a boot sektorů.

4.1.1 Techniky infekce Master Boot Recordu (MBR)

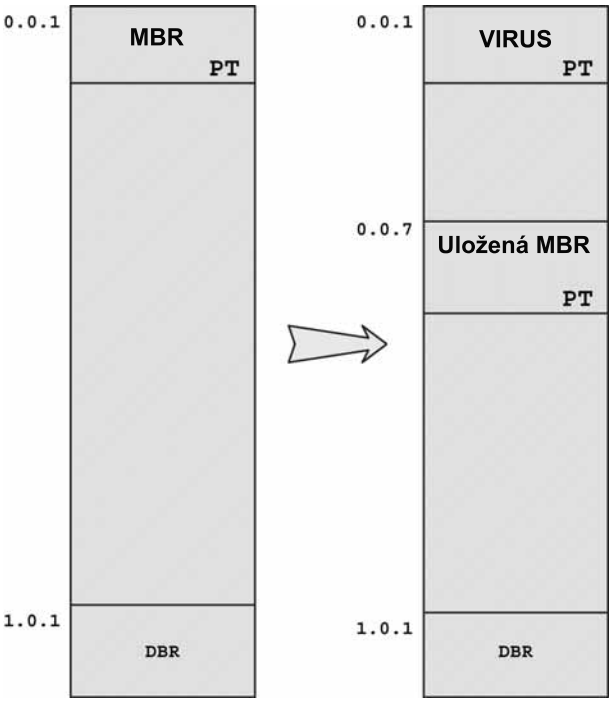
Infekce MBR je pro viry relativně jednoduchou úlohou. Velikost MBR je 512 bajtů, takže se do něj vejde jen malý kousek kódu, ale pro malé viry je to stále více než dost místa. Obvykle se MBR infikuje okamžitě po nabootování z infikované diskety z jednotky A:.

4.1.1.1 Infekce MBR nahrazením zavaděče

Klasický druh MBR virů používá k přístupu k diskům pro čtení a zápis službu BIOSu INT 13h. Většina MBR infektorů nahrazuje zavaděč umístěný na začátku disku svojí vlastní kopií a nezasahují do tabulky rozdělení disku. To je velmi důležité, protože když se bootuje z diskety, je pevný disk přístupný pouze tehdy, pokud je tabulka rozdělení disku svém na místě. V opačném případě pak nemá DOS žádnou možnost najít data na disku.

Virus Stoned je typickým představitelem používání této techniky. Virus uloží původní MBR na sektor 7 (viz obrázek 4.1). Jakmile se virus aktivuje díky nahrazení MBR, přečte původní uložený MBR ze sekto-

ru 7 do paměti a předá mu řízení. Těsně za MBR bývá většinou k dispozici pár prázdných sektorů a právě toho využívá virus Stoned. Na tuto výchozí podmínku se nicméně nedá stoprocentně spolehnout a to je přesně ten případ, kdy MBR viry po infekci znemožní korektní nabootování systému.



Obrázek 4.1 *Typické rozmístění disku před a po infekci virem Stoned.*

4.1.1.2 Nahrazení MBR kódu bez jeho uložení

Další virovou technikou k infekci MBR je ponechání tabulky rozdělení a přepsání zavaděče bez jeho úschovy. Takové viry potřebují zachovat funkčnost původního MBR – musí najít aktivní diskovou oblast, nahrát ji a posléze ji předat řízení.

Jedním z prvních virů, který začal používat tuto techniku, byl virus Azusa[2], který byl objeven v lednu 1991 v kanadském Ontariu. Takové viry nemohou být odstraněny běžnými metodami, protože není nikde zachována původní kopie MBR.

Antivirové programy rychle zareagovaly na toto nebezpečí přidáním standardního MBR kódu do svých produktů. Napadený počítač se pak vyléčil přepsáním virového kódu tímto kódem.

4.1.1.3 Infekce MBR změnou záznamu v tabulce rozdělení disku

Snadným cílem MBR infektorů je tabulka rozdělení disku. Změnou záznamu v této tabulce virus zajistí nahrání původního boot sektoru. MBR tedy nahraje zavirovaný boot sektor místo původního, přičemž původní boot sektor je nahrán virem ihned po jeho aktivaci. Virus StarShip je představitelem takové techniky. Některé viry, jako například někteří členové rodiny Ginger, mění záznamy v tabulce rozdělení disku tak, že dojde k zacyklení oblasti[3,4], což v případě MS-DOSu verze 4.0 až 7.0 způsobí, že počítač po nabootování skončí v nekonečné smyčce. Ke správnému nabootování z diskety je pak zapotřebí MS-DOS verze 3.3x nebo DOS systém jiný než od Microsoftu, jako například PC DOS.

4.1.1.4 Uložení MBR na konec pevného disku

Běžnou metodou infekce MBR je kompletní nahrazení MBR a uložení původní kopie na konec pevného disku, v naději, že jej nic nepřepíše. Některé opatrnější viry ještě zmenší velikost diskové oblasti a zabrání tím přepsání původního MBR. Tuto techniku například používá multipartivní (multipartite) virus Tequila.

4.1.2 Techniky infekce DOS BOOT Recordu (DBR)

Boot sektorové viry infikují první sektor disket, a případně i boot sektory pevných disků. Technik infekce boot sektoru je více než technik infekce MBR.

4.1.2.1 Standardní technika infekce boot sektoru

Jednou z nejpoužívanějších technik infekce boot sektoru vynalezly viry typu Stoned. Stoned infikuje boot sektor diskety nahrazením 512-bajtového boot sektoru svojí kopií a uložením původní kopie boot sektoru na konec kořenového adresáře.

V praxi je tato technika bezpečná jen do té doby, dokud není na disketě příliš mnoho souborů. Pak vede spuštění příkazu DIR k vypsání smetí na obrazovce.

4.1.2.2 Boot viry, které formátují dodatečné sektory

Některé boot viry jsou příliš velké na to, aby se vešly do jednoho sektoru. Většina disket se dá ovšem naformátovat tak, že se na ně vejde více dat, než je obvyklé při klasickém běžném formátování. Ne všechny disketové mechaniky umožňují formátování dodatečných sektorů, většina však ano. Například disketová mechanika mého prvního klonu IBM PC nepodporovala přístup na takto zformátované diskety. Výsledkem bylo to, že na mém systému nefungoval některý software s ochranou proti kopírování.

Některé ochrany proti kopírování totiž často využívají možnosti naformátovat na disketě dodatečné sektory umístěné mimo obvyklý rozsah. Proto obyčejné nástroje na kopírování disket, jako třeba DISKCOPY, nedokáží vytvořit identickou kopii dat.

Některé viry speciálně naformátují několik sektorů na disketě, aby znemožnily antivirovým programům přístup k původní kopii boot sektoru. Hlavním důvodem používání této techniky je nicméně hlavně to, že virus je příliš velký.

Indonéský virus Denzuko je představitelem této techniky. Denzuko byl vypuštěn během jara roku 1988 a narozdíl od jiných virů je znám jeho autor – napsal jej Denny Yanuar Ramdhani. Přezdívka autora byla Denny Zuko, která pochází ze jména "Danny Zuko", což byl hlavní hrdina oblíbeného filmového muzikálu Pomáda, kterého hrát John Travolta[5]. Tento boot virus byl mezi prvními, který začal útočit na jiné počítačové viry. Denzuko odstraňoval virus Brain, pokud jej našel v počítači.

Denzuko se také uměl projevovat (rutinám starajícím se o cílený projev viru říkáme payload) – po stisku kláves Ctrl-Alt-Del na zlomek sekundy zobrazil tento obrázek a poté provedl restart počítače, přičemž nadále zůstal v paměti[6].

Obrázek 4.2 *Payload viru Denzuko.*

Tuto techniku používá také velmi složitý a nebezpečný maďarský stealth BOOT/MBR virus Töltögetö (známý též jako Filler). Vytvořil jej jeden student výpočetní techniky na střední škole v Székesfehérváru v Maďarsku v roce 1991. Filler formátuje diskety o kapacitě 360 kB a 1.2 MB – konkrétně sektory na stopě 40 nebo 80. Tyto oblasti disket obvykle nebývají naformátované.

Výhodou tohoto druhu techniky infekce je možnost oživení mrtvého virového kódu. První oživovací pokusy byly u virů objeveny na počátku 90. let. Například některé COM infektory se pokoušely umístit sama sebe k těsnému konci disku mimo obvykle formátované oblasti a pak předaly řízení nahranému sektoru. Většina prvních antivirových řešení při procesu léčení nepřepisovala celý virový kód, zejména ne ten kód, který byl umístěn na disku mimo obvyklý rozsah. Antivirové programy opravily pouze boot sektor, přičemž odstřihnutý virový kód byl považován za mrtvý. Ovšem, někteří autoři virů toho využili a mrtvý kód viru oživili prostřednictvím jiného viru.

4.1.2.3 Boot viry, které označují sektory za vadné

Zajímavou metodou některých boot virů je nahrazení původního boot sektoru virovým kódem a uložení původní kopie nebo další části viru do prázdného clusteru, který se poté ve FAT tabulce označil jako vadný. Představitelem této virové techniky je nebezpečný Disk Killer, který byl vytvořen v dubnu v roce 1989[7].

4.1.2.4 Boot viry, které neukládají původní boot sektor

Některé boot viry vůbec neukládají původní boot sektor diskety a místo toho napadají aktivní boot sektor nebo MBR pevného disku, aby pak předaly řízení uloženým boot sektorům na pevném disku. Infekce na disketě tak nemůže být opravena standardními technikami, neboť virus nepotřebuje ukládat původní boot sektor. Protože je boot sektor specifický pro konkrétní operační systém, není proces léčení tak jednoduchý, jako v případě nahrazení MBR kódu – pro jednotlivé OS totiž existuje mnoho odlišných boot sektorů OS. Většina antivirových řešení řeší tento problém tak, že přepíší virový kód kódem standardního boot sektoru, který zobrazí výzvu uživateli, zda-li se má nabootovat z pevného disku. Výsledkem je, že se disketa nedá uvést stoprocentně do původního stavu.

Druhou, méně obvyklou metodou je přepsání boot sektoru diskety virovým kódem, který napadne MBR nebo boot sektor pevného disku. Virus potom zobrazí falešnou hlášku, něco ve stylu "Non-system disk or disk error" a nechá uživatele načíst virus z pevného disku. Tuto techniku například využívá virus Strike.

Další metodou infekce boot sektoru disket bez uložení originálu je předstírání funkčnosti boot sektoru a načtení některých systémových souborů, což ovšem funguje pouze za předpokladu, že se virus strefí do správného operačního systému. Takhle to například dělá virus Lucifer.

4.1.2.5 Boot viry, které ukládají původní boot sektor na konec disku

Další kategorie boot virů nahrazuje původní boot sektor přepsáním virovým kódem a uložení jeho kopie na konec pevného disku. Slavným představitelem této techniky je virus Form, který ukládá originální boot sektor na těsný konec disku. Form předpokládá, že se tento sektor téměř vůbec nepoužívá, a může tak sloužit jako vhodné místo na uložení kopie s nízkým rizikem pozdějšího přepsání. Virus tedy nepotřebuje nijak označovat tento sektor, a ani měnit velikost diskové oblasti.

Jiné boot viry také ukládají boot sektor na konec aktivní diskové oblasti a navíc zmenšují její velikost tak, že sektor s původní kopií se nebude pro systém tvářit jako volný – nedojde tedy k jeho nechtěnému přemazání. Eventuálně je možné ze stejného důvodu pozměnit datovou oblast boot sektoru.

4.1.3 Boot viry, které dovedou pracovat s Windows 95

Několik boot virů, obvykle multipartitního charakteru, útočí na ovladač disketové mechaniky, který je uložený v \SYSTEM\IOSUBSYS\HSFLOP.PDR. Tato technika se prvně objevila ve slovinské rodině virů nazvané jako Hare (nebo také Krishna) v květnu roku 1996, kterou napsal Demon Emperor.

Viry odstraňují tento soubor z toho důvodu, aby získaly přístup k obsluze služby BIOSu INT 13h, pokud systém obsahuje aktivní Windows 95. Bez tohoto triku by totiž boot viry nemohly infikovat diskety prostřednictvím volání INT 13h, protože by pro ně nebylo toto volání dostupné.

4.1.4 Možné útoky boot virů v síťovém prostředí

Bezdiskové pracovní stanice bootují prostřednictvím souboru uloženého na serveru. Například na serverech Novell NetWare existuje příkaz DOSGEN.EXE, který dovede vytvořit obraz bootovací diskety

NET$DOS.SYS pro použití na terminálech. Ty mají speciální EPROM čip, který umí na síti najít bootovací image.

To nabízí útočníkovi dvě možnosti. Ta první je infekce nebo nahrazení souboru NET$DOS.SYS na serveru v okamžiku, kdy je k němu umožněn přístup. Druhou možností je simulace funkčnosti serverového kódu a hostování falešných virtuálních serverů prostřednictvím virového kódu umístěného na síti.

Takové viry zatím nejsou známy, nicméně soubor NET$DOS.SYS bývá často infikován a zůstává nepostřehnut mnoha antivirovými skenery.

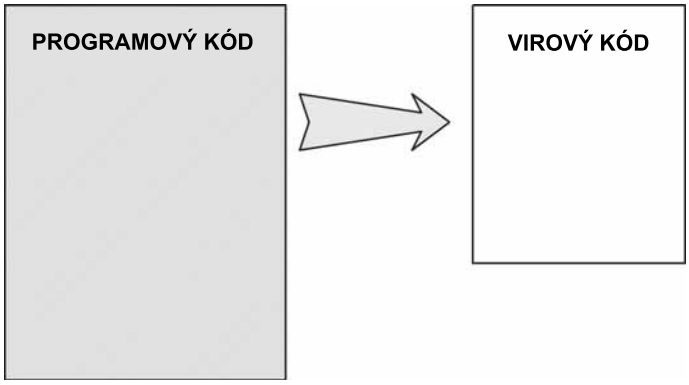
4.2 Techniky infekce souborů

V této části se dozvíte o běžných metodách infekce souborů, které autoři[8] virů léta používali k nabourání se do hostitelských systémů.

4.2.1 Přepisující viry

Některé viry jednoduše najdou vhodný soubor na disku a přepíší ho vlastní kopií. Jedná se o velmi primitivní techniku, která se však nejsnadněji implementuje. Takové jednoduché viry dovedou napáchat velkou škodu, pokud přepíší soubory na celém disku.

Soubory napadené přepisujícími viry nemohou být vyléčeny a musí být smazány z disku a následně obnoveny ze záloh. Následující obrázek 4.3 ukazuje, jak se změní obsah hostitelského programu po napadení takovým virem.



Obrázek 4.3 *Přepisující virus, který mění velikost hostitele.*

Přepisující viry nejsou obvykle příliš úspěšné, protože vedlejší efekty jejich činnosti uživatelé rychle objeví. Takové viry mají nicméně větší šířící potenciál, zejména tehdy, pokud se tato technika zkombinuje s technikou šíření po síti. Například virus VBS/LoveLetter.A@mm odesílá sebe sama na jiné systémy prostřednictvím elektronické pošty. Po své aktivaci přepíše svojí kopií všechny soubory s těmito příponami:

.vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .wav, .txt, .gif, .doc, .htm, .html, .xls, .ini, .bat, .com, .avi, .qt, .mpg, .mpeg, .cpp, .c, .h, .swd, .psd, .wri, .mp3 a .mp2.

Jinou metodou infekce přepisem používají takzvané "mrňavé" (tiny) viry. Typickou rodinou tohoto typu infektorů je rodina Trivial pro operační systém DOS. Během počátku 90. let se mnoho autorů počítačových virů pokoušelo napsat co nejmenší možný virus. Není tedy překvapením, že existuje mnoho variant viru Trivial. Některé z nich jsou dlouhé pouhých 22 bajtů (Trivial.22).

Algoritmus takových virů je velmi jednoduchý:

1. Vyhledat libovolný soubor (*.*) v aktuálním adresáři.
2. Otevřít soubor pro zápis.
3. Zapsat tělo viru na začátek hostitelského souboru.

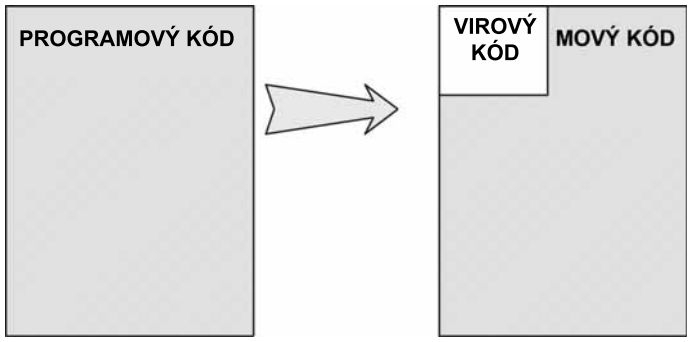
Tyto nejkratší viry často nedovedou infikovat více než jeden soubor v aktuálním adresáři – z toho důvodu, že kód na vyhledání dalšího hostitelského souboru by zabral o pár bajtů víc. Takové viry nejsou dostatečně vyvinuty na to, aby byly schopny infikovat soubory určené pouze pro čtení – opět proto, že by to vyžadovalo pár instrukcí navíc.

Virový kód bývá často optimalizován tak, aby využíval nastavení registrů dle konkrétního operačního systému – virus tedy nemusí inicializovat registry, jejichž obsah je předem známý. Díky tomu mohou autoři ještě více zkrátit délku svých virů.

Takové optimalizace mohou nicméně způsobit fatální chyby, pokud se virus spustí na platformě, která registry inicializuje na jiné hodnoty, než jaké virus očekával.

Některé šikovné přepisující viry také používají služeb BIOSu pro zápis sektorů místo DOSových souborových funkcí. Nejprimitivnější forma takového viru byla implementována na 15 bajtů. Virus přepíše každý sektor na disku sebe samým. Poškození systému, ke kterému dojde, je tak závažné, že svou aktivitou velmi záhy zlikviduje hostitelský systém.

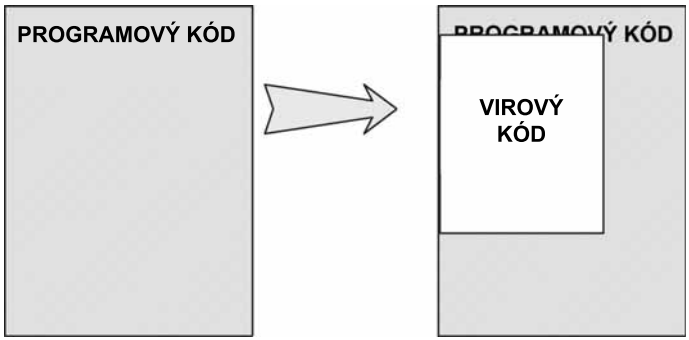
Obrázek 4.4 názorně ukazuje přepisující virus, který jednoduše přepíše svým tělem začátek hostitele, přičemž nijak nezmění jeho velikost.



Obrázek 4.4 *Přepisující virus, který nemění velikost hostitelského programu.*

4.2.2 Náhodně přepisující viry

Další neobvyklá varianta přepisovací techniky nemění kód programu na jeho začátku – místo toho si náhodně vybere oblast uprostřed souboru, na kterou se zapíše. Virový kód se nemusí za každou cenu aktivovat během spouštění hostitele, ten je ale každopádně nenávratně poškozen a může havarovat už před samotnou aktivací viru. Příkladem takového viru je Omud[9], zobrazený na obrázku 4.5.



Obrázek 4.5 *Náhodně přepisující virus.*

Pro vylepšení výkonu omezením I/O operací jsou moderní antivirové programy optimalizovány tak, aby byly schopny nalézt viry na známých místech. Náhodně přepisující viry jsou problémem pro skenery, protože ty pak potřebují zanalyzovat kompletní obsah hostitele, což je časově a výkonově náročné.

4.2.3 Připojující viry

Typickou technikou infekce DOSových COM souborů je vložení instrukce skoku (JMP) na začátek hostitele, která směřuje přesně na jeho konec. Příkladem může být virus Vienna, jehož lehce upravená varianta byla publikována v knize o počítačových virech Ralfa Burgera společně se zdrojovými kódy v letech 1986-87.

Tato technika má své pojmenování podle umístění virového těla, které se připojí na konec hostitele. Je zajímavé, že některé viry infikují EXE soubory tak, že je nejprve převedou na COM. Tuto techniku například používá rodina viru Vacsina.

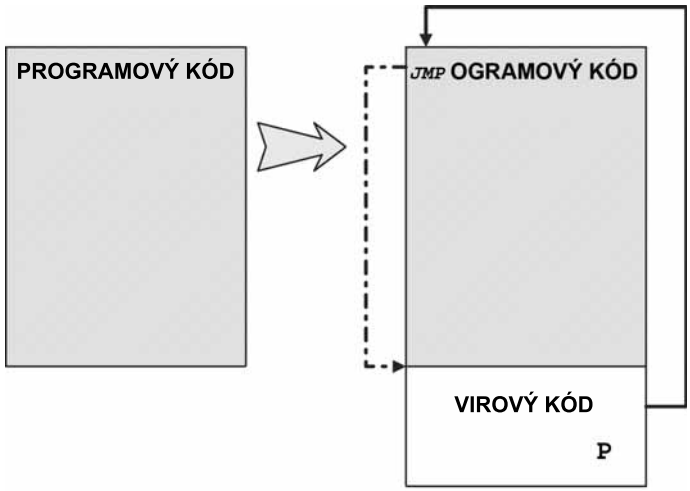
Instrukce skoku je někdy nahrazena instrukcemi se stejnou funkčností, jako například těmito:

```
a.) CALL zacatek_viru
b.) PUSH offset zacatek_viru
    RET
```

První tři přepsané bajty na začátku hostitelského programu jsou uloženy ve virovém těle. Jakmile dojde ke spuštění infikovaného programu, virus načte hostitele do paměti, instrukce skoku přesměruje vykonávání do těla viru, kde typicky dojde k replikaci vyhledáním dalších vhodných souborů k infekci nebo ke spuštění aktivační rutiny a konečně k obnovení hostitele zkopírováním původních bajtů na začátek programu (offset CS:0x100, což je paměťová adresa, na kterou systém nahrává COM soubory) a skokem

zpět na CS:0x100. Soubory COM se nahrávají na tuto adresu proto, že prefix segmentu programu (*program segment prefix*, PSP) je umístěn na CS:0 - CS:0xFF.

Obrázek 4.6 znázorňuje, jak připojující COM virus infikuje hostitelský program.



Obrázek 4.6 *Typický způsob infekce připojujícím virem.*

Technika připojení na konec souboru se dá implementovat pro libovolný typ spustitelného souboru, například pro EXE, NE, PE, ELF atd. Takové soubory mají hlavičku, která obsahuje adresu hlavního vstupního bodu, který je většinou nahrazena novým vstupním bodem, kterým je začátek virového kódu, připojeného na konec hostitele.

Část 4.3 je věnovaná technikám infekce systému Win32 a demonstruje principy technik infekce moderních souborových formátů. Tyto formáty mají obvykle složité interní struktury a nabízející útočníkům více možností.

4.2.4 Viry připojující se na začátek souboru

Tato častá technika infekce je založena na principu vložení virového kódu na začátek hostitele. Takové viry nazýváme jako viry připojující se na začátek hostitele, neboli prependery. Jedná se o jednoduchý, avšak úspěšný způsob infekce, který autoři virů implementovali na různých operačních systémech.

Příkladem takového viru je maďarský virus Polimer.512.A, který na začátek hostitele připojuje svůj 512 bajtů dlouhý kód, a který posune obsah hostitelského souboru tak, aby jej následoval.

Podívejme se na začátek tohoto viru v DOSovém DEBUGu. Polimer je vhodným příkladem, protože začátek viru obsahuje neškodnou datovou oblast se zprávou, která se zobrazí během spuštění infikovaných programů.

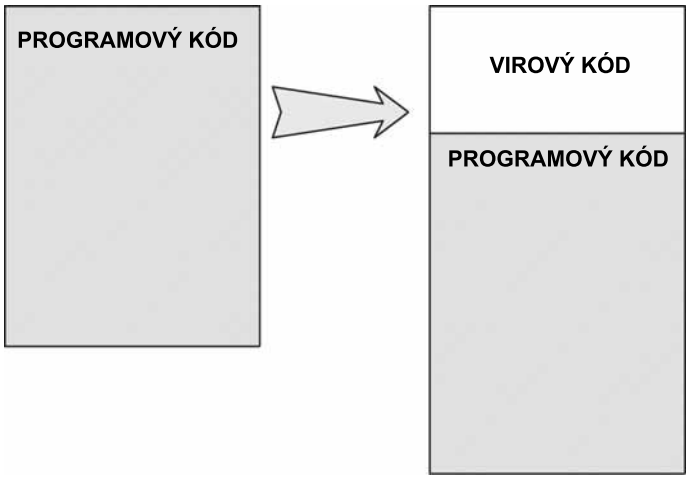
```
>DEBUG polimer.com
-d
142F:0100  E9 80 00 00 3F 3F 3F 3F-3F 3F 3F 3F 43 4F 4D 00   ....????????COM.
```

```
142F:0110  05 00 00 00 2E 8B 26 68-01 00 00 00 00 00 00 00   ......&h........
142F:0120  00 00 00 00 00 00 00 00-41 20 6C 65 27 6A 6F 62   ........A le'job
142F:0130  62 20 6B 61 7A 65 74 74-61 20 61 20 50 4F 4C 49   b kazetta a POLI
142F:0140  4D 45 52 20 6B 61 7A 65-74 74 61 20 21 20 20 20   MER kazetta !
142F:0150  56 65 67 79 65 20 65 7A-74 20 21 20 20 20 20 0A   Vegye ezt ! .
```

Virové tělo se nahraje do paměti na offset 0x100. Kód začíná instrukcí skoku (0xe9), která předá řízení virovému kódu, jenž následuje za datovou oblastí. Protože je Polimer 512 bajtů (0x200) dlouhý, bude offset hostitelského programu v paměti tento: 0x300 (0x100+0x200=0x300). A skutečně, v naší ukázce je infikovaný program Free Memory Query. COM prependery mohou jednoduše spustit hostitelský program tak, že zkopírují původní obsah programu na offset 0x100 a předají mu řízení.

```
-d300
142F:0300  E9 9E 00 0D 46 72 65 65-20 4D 65 6D 6F 72 79 20   ....Free Memory
142F:0310  51 75 65 72 79 20 50 72-6F 67 72 61 6D 2C 20 56   Query Program, V
142F:0320  65 72 73 69 6F 6E 20 34-2E 30 33 0D 0A 53 4D 47   ersion 4.03..SMG
142F:0330  20 53 6F 66 74 77 61 72-65 0D 0A 28 43 29 20 43    Software..(C) C
142F:0340  6F 70 79 72 69 67 68 74-20 31 39 38 36 2C 31 39   opyright 1986,19
142F:0350  38 37 20 53 74 65 76 65-6E 20 4D 2E 20 47 65 6F   87 Steven M. Geo
142F:0360  72 67 69 61 64 65 73 0D-0A 1A 00 00 00 00 00 00   rgiades.........
```

Obrázek 4.7 demonstruje, jak se prepender vkládá na začátek programu.



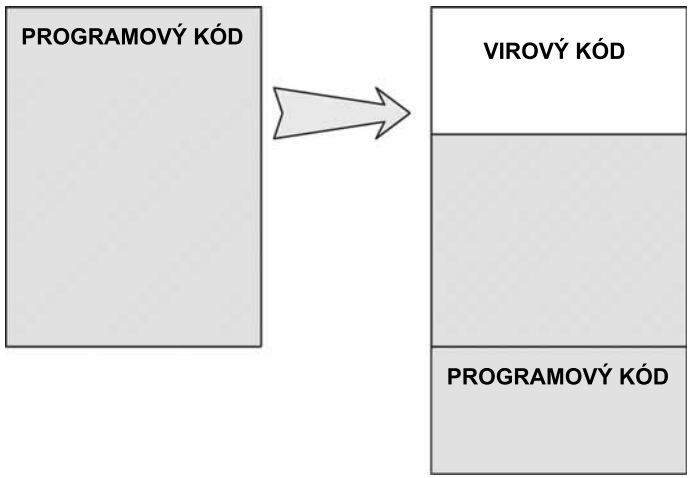
Obrázek 4.7 *Typický virus, který se připojuje na začátek hostitele.*

Prependery bývají obvykle napsány v pokročilých programovacích jazycích, jakým je třeba jazyk C, Pascal nebo Delphi. V závislosti na aktuální struktuře spustitelného souboru nemusí být infekce programu tak triviální, jako v případě COM souborů. Přesně z tohoto důvodu viry na disku vytváří dočasný soubor, který obsahuje původní hostitelský program, přičemž pro jeho spuštění se použije funkce typu system(). Takové viry obvykle předají parametry příkazové řádky původnímu programu a tím zachovají funkčnost aplikace, která by mohla být narušena chybějícími parametry.

4.2.5 Klasické parazitické viry

Variantou techniky připojení na začátek souboru je technika známá jako klasická parazitická infekce, znázorněná na obrázku 4.8. Takové viry přepíší začátek hostitele vlastním kódem a uloží jej na jeho úplný konec, obvykle na offset délky viru. První takový virus byl Virdem, napsaný Ralfem Burgerem. Ve skutečnosti je Virdem jedním z prvních příkladů souborových virů, který byl zaznamenán; Burgerova kniha nikdy neobsahovala informace o jiných než souborových virech. Burger rozšířil svůj výtvor na konferenci Chaos Computer Clubu v prosinci roku 1986.

Často se po vyléčení takto zavirovaných souborů objeví obvyklé problémy. V mnoha případech se oprava provede tak, že se zkopíruje N bajtů na začátek souboru a soubor se zkrátí o velikost souboru mínus N, kde N je typicky velikost viru (ovšem délka souboru se může měnit). Nejčastější příčinou nekorektního léčení je mnohonásobná infekce, tedy situace, kdy je soubor infikován více než jednou.



Obrázek 4.8 *Klasický parazitický virus.*

V jiných případech má soubor na svém konci nějaká speciální data, jako například dodatečné informace vložené nějakým antivirovým programem. Například virus Jerusalem používal značku MS-DOSu umístěnou na konci souboru, aby rozeznal soubory, které jsou už infikované. Některé z prvních antivirových programů připojovaly na konec všech COM a EXE programů tento řetězec, aby tak zamezily opětovné infekci Jerusalemem. Ačkoliv to může znít jako dobrý nápad, takové změny souborů mohou dezinfekčním programům způsobit problémy. K tomu může dojít třeba v případě, že takto označený soubor byl už napaden jiným parazitickým virem. Jestliže se pro vyléčení souboru použije výpočet "velikost souboru-N", sáhne opravná rutina třeba o 5 bajtů dál za původním programem. Toto léčení pak bude mít za následek poškození programu, který zhavaruje po každém svém spuštění. Tomuto druhu dezinfekce se říká "rychlokvašená oprava" (half-cooked repair[10]).

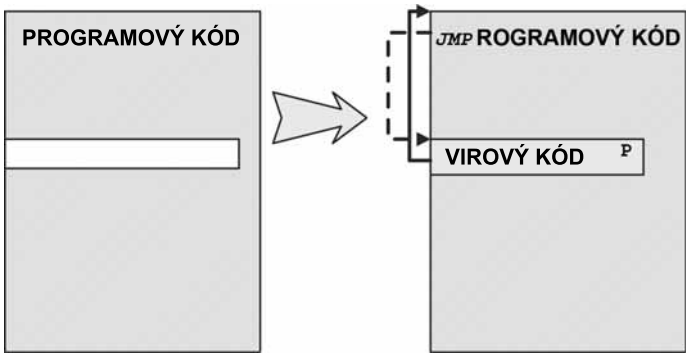
Některé speciální parazitické infektory neukládají začátek hostitele na jeho konec a místo toho používají dočasný soubor k uložení této informace mimo hostitele, někdy se skrytými atributy. Například maďarský DOS virus Qpa tuto techniku používá a ukládá 333 bajtů (velikost viru) do speciálního souboru.

Tuto techniku používají také členové nechvalně známé rodiny virů W32/Klez pro uložení celého hostitelského programu v novém souboru.

4.2.6 Dutinové viry

Dutinové viry (cavity viruses), znázorněné na obrázku 4.9, obvykle nezvětšují velikost svého hostitele. Místo toho přepíší určitou oblast souboru, do které se mohou bezpečně vložit. Tyto infektory většinou přepisují oblasti binárních souborů, které obsahují nuly, nicméně mohou přepsat i bloky 0xCC, které často používají kompilátory jazyka C pro zarovnání instrukcí. Jiné viry zase přepisují oblast s mezerami (bajty 0x20).

Prvním virem, který začal používat tuto techniku, byl Lehigh v roce 1987. Lehigh byl vcelku neúspěšný virus, nicméně Ken van Wyk zajistil viru mnoho publicity a vytvořil na Usenetu diskusní skupinu VIRUS-L, aby s ostatními prodiskutoval svoje poznatky.



Obrázek 4.9 *Mezerový virus, který sám sebe vkládá do mezery v hostiteli.*

Dutinové viry obvykle bývají DOS infektory s pomalým šířením. Například bulharské viry Darth Vader nikdy nepůsobily velké škody, především kvůli faktu, že se jedná o pomalý infektor. Vždy počkal, až se program sám zapíše a teprve pak na něj zaútočil.

Virus W2K/Installer (autoři Benny a Darkman) používá tuto techniku k infekci Win32 PE souborů na Windows 2000 bez zvětšování jejich velikosti.

Speciální druh těchto virů zneužívá relokační sekce PE programů. Relokace spustitelných souborů ve většině případů nejsou zapotřebí a novější linkery dovedou zkompilovat spustitelné PE soubory bez relokačních tabulek, čímž tak zmenšit velikost výsledného programu. Dutinové viry útočící na relokace přepíší relokační sekci (pokud ji v programu naleznou). Jestliže je relokační sekce menší než virový kód, virus velikost souboru nezvětší, protože soubor jednoduše nenapadne. Takové viry si pečlivě ověřují, jestli je relokační sekce dostatečně velká nebo zdali je alespoň poslední v pořadí, jinak by došlo k poškození souboru. Tuto techniku například používají rodiny virů W32/CTX a W95/Vulcano.

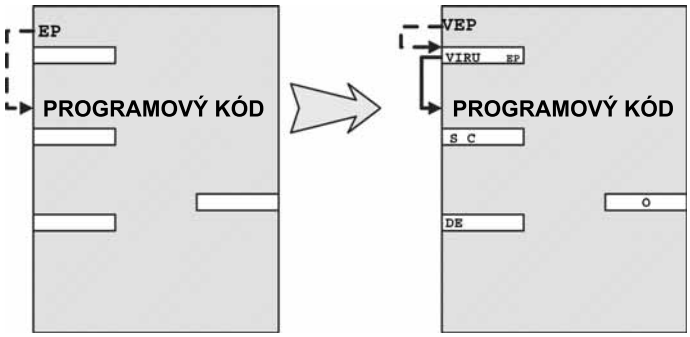
4.2.7 Dělené dutinové viry

Několik virů pro Windows 95 používá dutinovou techniku infekce extrémně úspěšným způsobem, příkladem může být například virus W95/CIH. Jeho virový kód je rozdělený na zaváděcí rutinu a N sekcí. Zaváděcí rutina (hlavička) viru nejprve nalezne zbylé části virového kódu a načte je do spojité paměti (s pomocí tabulky offsetů, která je uložena v hlavičce). Při infikování virus nejprve najde dostatek prázdných míst v PE souboru a do nich pak nakopíruje jednotlivé části kódu.

Nový vstupní virový bod bude zaznamenán v hlavičce souboru a bude ukazovat na začátek virového kódu, který je obvykle umístěný někde uprostřed hlavičky hostitele. Některé kratší dutinové infektory, jako je třeba Murkry, používají tuto oblast k infekci souborů v jednom kroku. CIH je nicméně delší a potřebuje svůj kód rozdělit do menších částí. Virus spustí hostitelský program skokem na původní uložený vstupní bod. Výhodou této techniky je to, že si virus potřebuje zapamatovat pouze původní vstupní bod hostitele. V načteném programu pak pouze stačí skočit na tu správnou adresu.

Obrázek 4.10 znázorňuje stav hostitelského programu před a po infekci děleným dutinovým virem. Hostitel by normálně začal na svém vstupním bodu, který je definovaný v hlavičce. Virus nahradí tento bod virovým vstupním bodem, který ukazuje na začátek zavaděče, který poté načte zbývající části kódu. V případě, že v souboru není dostatek místa pro uložení celého zavaděče do jedné části kódu, infekce neproběhne.

V moderních souborových formátech, jakým je třeba PE, bývají mezery k dispozici a dají se jednoduše najít s použitím informací uložených v hlavičkách sekcí.



Obrázek 4.10 *Dělený dutinový virus.*

Jedním ze speciálních problémů těchto virů je skutečnost, že obsah přepsaných oblastí nemůže být stoprocentně obnoven. K tomu dochází hlavně v případě virů, které přepíší oblast souboru, která obvykle obsahuje nuly, nicméně v tomto konkrétním případě obsahuje něco jiného. Potom nebudou kryptografické kontrolní součty po vyléčení souboru odpovídat. Také se zkomplikuje přesná identifikace takových virů, protože je nutné, aby byly kousky kódu poskládány dohromady.

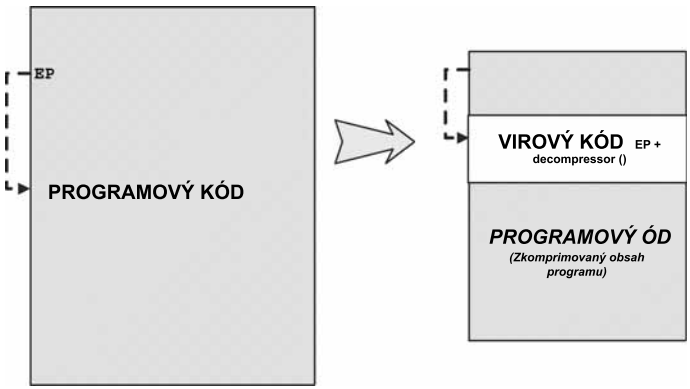
Detekce takových virů je založena na obsahu zaváděcí rutiny, která musí být uložena v jediné části kódu.

4.2.8 Komprimující viry

Tato speciální virová technika využívá možnosti zkomprimovat obsah hostitelského programu. Binární zkomprimování hostitele se někdy používá pro skrytí nárůstu délky infikovaného souboru. Komprimující viry se občas nazývají "užitečnými" ;-), protože dovedou zkomprimovat svého hostitele o mnoho více, než jej prodloužit, čímž šetří místo na disku. Tzv. runtime komprimační programy, jako PKLITE, LZEXE, UPX nebo ASPACK, jsou velmi oblíbené, nicméně jsou často zneužívány útočníky pro zkomprimování trojských koní, počítačových virů a červů tak, aby byly menší a daly se hůře analyzovat.

DOSový virus Cruncher byl první, který přišel s kompresní technikou. Některé 32bitové viry pro Windows ji také používají, jako třeba W32/HybrisF (souborový infektor červa Hybris ve formě plug-inu), jehož autor si říká Vecna. Dalším nechvalně známým představitelem je W32/Aldebera, který kombinuje metody infekce s polymorfismem. Aldebera se snaží zkomprimovat hostitele tak, že jeho velikost zůstane po infekci stejná. Byl vytvořen v roce 1999 členem virové skupiny IKX B0/S0 (Bozo).

Virus W32/Redemption napsaný Jackem Qwertmy také používá kompresní techniku k infekci 32bitových PE souboru na Windows. Obrázek 4.11 znázorňuje, jak komprimující viry útočí na soubory.



Obrázek 4.11 *Komprimující virus.*

4.2.9 Infekce typu Amoeba

Amoeba je typ neobvyklé techniky infekce, která připojuje hostitelský program doprostřed virového těla. To se učiní připojením hlavičky viru na začátek a konec hostitele. Původní program se zrekonstruuje, uloží a spustí jako nový soubor na disku. Tuto techniku používá k infekci PE souborů na systémech Windows například virus W32/Sand.12300, vytvořený autorem Alcopaul a naprogramovaným ve Visual Basicu.

Na obrázku 4.12 je vidět hostitelský program před a po infekci virem, který používá techniku Amoeba.