Druhy virů

Boot viry
napadají systémové oblasti disku. I přesto, že je jich méně než souborových virů, vyskytují se častěji. Šíří se následujícím způsobem: když restartujete počítač, který má povoleno zavádění systému z disketové mechaniky a v mechanice je disketa s boot virem, vir se spustí a napadne systémové oblasti pevného disku. Při dalším spuštění počítače se boot vir inicializuje z pevného disku a napadá diskety, které uživatel použije.

Souborové viry
napadají pouze soubory. Přesněji řečeno soubory, které obsahují prováděný kód - programy. V napadeném programu přepíší část kódu svým vlastním, nebo vlastní kód k programu připojí a tím změní jeho velikost a chování.

Multipartitní viry
napadají soubory i systémové oblasti disku. S výhodou kombinují možnosti boot virů i souborových virů.

Makroviry
napadají datové soubory - dokumenty vytvořené v některých kancelářských aplikacích. Využívají toho, že tyto soubory neobsahují pouze data, ale i makra, která viry využívají ke svému šíření. Jsou napadány především dokumenty aplikací MS Office, výjimečně byly zaznamenány i případy dokumentů jiných aplikací. Možnosti jazyka Visual Basic for Aplications, ve kterém jsou psána makra v MS Office 97, jsou velmi rozsáhlé a bezpečnost je minimální. V nedávné době se o tom mohly přesvědčit oběti viru W97M Melissa, který při své aktivaci použije dokument, na němž uživatel zrovna pracuje, infikuje jej a rozešle elektronickou poštou na 50 náhodně vybraných adres z uživatelova adresáře. Následky takové akce pravděpodobně nebudou fatální, ale podobný makrovirus může například vykrádat z vašeho počítače důvěrné informace, pracovat s vašimi soubory, spouštět aplikace.

Makroviry jsou v současné době nejčastěji se vyskytující druh viru. Jsou také největší hrozbou do budoucna. Opatrný uživatel sice může omezit množství spustitelných souborů, které si kopíruje na počítač, ale výměně elektronických dokumentů se nevyhne.

Stealth viry
jsou viry, které se chrání před detekcí antivirovým programem použitím tzv. stealth technik: pokud je takový virus v paměti, pokouší se přebrat kontrolu nad některými funkcemi operačního systému a při pokusu o čtení infikovaných objektů vrací hodnoty odpovídající původnímu stavu.

Polymorfní viry

se pokouší znesnadnit svou detekci tím, že mění vlastní kód. V napadeném souboru není možné najít typické sekvence stejného kódu.

Rezidentní viry
zůstávají po svém spuštění přítomny v paměti.

Retro viry - odvetné viry
Hlavním heslem těchto virů je: nejlepší obrana je útok. A to taky dodržují. Snaží se obejít a ještě lépe znemožnit práci antivirovým programům. Proto je mažou, vypínají rezidentní ochrany apod. Pozornost si zaslouží virus Tequila, který odstraňuje kontrolní součty přidané pomocí Viruscanu přímo ze souborů.