Utekly kódy – je to pohroma!

Část zdrojových kódů operačních systémů Windows NT4 a 2000 se dostala na internet

VOJTĚCH BEDNÁŘ

Letošní únorový pátek třináctého byl, přinejmenším pro společnost Microsoft Corporation, vskutku nešťastným dnem. Došlo totiž k neautorizovanému zveřejnění části zdrojových kódů operačních systémů Windows NT4 a 2000. Co vše to může znamenat pro svět a pro internet, nebo pro telekomunikace vůbec? Znamená to hodně. První zprávy hovořily o tom, že vyzrazené kódy představují pouze malou část celých Windows. Posléze se ale ukázalo, že zhruba dvousetmegabajtový archiv obsahuje velké množství podstatných komponent tvořících OS. Z toho, co uteklo, sice není možné zkompilovat funkční Windows, ale to není příčinou, proč kódy zmizely.

Zdrojový kód

Prakticky každý program a operační systém je vlastně velice složitá sada počítačových programů, a může existovat ve dvou podobách. První z nich tvoří zkompilovaný binární (pseudobinární) kód. To jsou všechny ty soubory s příponami .exe, .dll, .sys a další. Právě ony mohou fungovat, mohou být spuštěny a vykonávat nějakou činnost. Proto se distribuují uživatelům.

Kromě toho ale každý program existuje ve formě takzvaných zdrojových kódů nebo textů. Jsou to skutečně textové soubory obsahující struktury programovacího jazyka, ve kterém je program napsán. Teprve po zpracování těchto textů aplikací nazvanou Kompilátor je vytvořen například náš soubor .exe, který již lze běžným způsobem spustit a provozovat.

Zkompilovaný kód lze spustit, ale není jej možno změnit. Všechny změny v programu nebo jeho modulu (s výjimkou některých, pokud to program umožňuje) je proto třeba provádět v jeho zdrojových textech. Aby se jakákoliv změna promítla do fungujícího programu, musí být po jejím provedení znovu zkompilován. Proto jsou zdrojové kódy tak chráněným a cenným zbožím, tedy alespoň pro společnosti tvořící proprietární software, mezi něž se řadí i Microsoft.

Kód ve službách zločinu

Uteknuvší zdrojové texty Windows mohou být snadno zneužity proti jejich autorům a především uživatelům. Předpokládá se, že kód obsahuje množství chyb. Na některé lze přijít i z jeho zkompilované podoby, jiné jsou naopak zřejmé pouze ze zdrojového textu. Pokud tento text máme k dispozici, můžeme takové chyby odhalit a zneužít je například k průniku do zabezpečeného operačního systému. Stejně tak jimi může být systém zastaven, restartován, anebo výrazně pozměněna jeho funkčnost. To je ohromné riziko, kterého si je výrobce velmi dobře vědom. Ukradené kódy sice patří dnes již zastaralým systémům, respektive jejich verzím, avšak i tak se vyskytují i v nových OS Windows XP a připravovaném systému Longhorn, stejně tak jako ve Windows Serveru 2003. Díky tomu se riziko přesouvá i na tyto operační systémy. Všechny červy, kterým se až doposud povedlo masivní rozšíření, s jedinou významnou výjimkou, vyžadovaly být spuštěny uživatelem. Znalost zdrojových kódů však otevírá cestu k novým, dokonalejším škodlivým kódům. Takovým, které se podobně jako loňský Blaster mohou do OS dostat jinak než e-mailem, formou přímého útoku. Navíc hrozí, že záplatování využité chyby bude ztíženo její složitostí, nebo že takový škodlivý kód bude využívat důležitých služeb, které nelze dost dobře změnit.

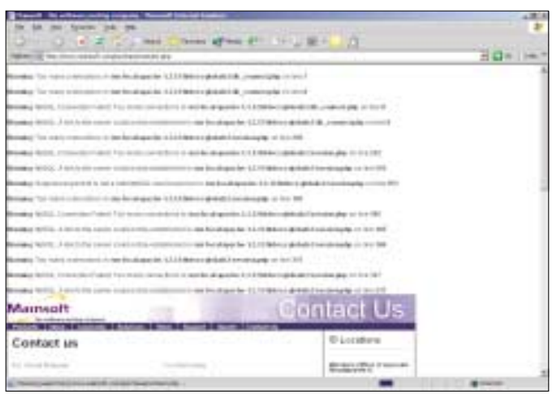
Kód ve službách lidstva

Existují ovšem i pozitivní věci spojené s útěkem zdrojového kódu z Microsoftu. Především programátoři, kteří se ke zdrojovým kódům (ilegálně) dostali, se mohou konečně podívat, jak Windows uvnitř ve skutečnosti pracují. V důsledku toho mohou být jejich aplikace lépe naprogramované. Mohou také lépe využívat vnitřních služeb operačního systému, díky tomu běžet rychleji, lépe a být méně poruchové. Nedostatky, které vyplynou kvůli nechtěnému zveřejnění kódů na povrch, mohou být opraveny dříve, než jsou zneužity. Už samotný fakt, že se zdrojové texty dostaly na veřejnost, donutil výrobce systému k masivní vlně prověření jeho bezpečnosti, k preventivnímu vyhledávání možných slabých míst. Dá se předpokládat, že texty využije ke stejné činnosti také mnoho dalších dobrovolníků, a tak se to, k čemu došlo, může stát vlastně užitečným jak uživatelům, tak v konečném důsledku i Microsoftu.

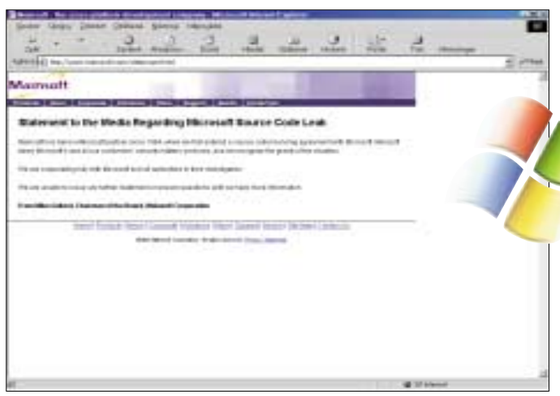
Klon na cestě?

O klonování lidí se vedou dalekosáhlé spory, ale jak je to s klonováním operačního systému? Jak už bylo řečeno, z toho, co uteklo, funkční Windows neuděláme. Přesto mohou být texty využity při tvorbě řekněme nového operačního systému, nebo při vývoji současných napodobenin. Například pod operačním systémem Linux lze již nyní provozovat některé aplikace pro Windows, včetně například Microsoft Office. Poznání původních zdrojových textů bude mít pravděpodobně za následek zdokonalení technologií, jež toto umožňují, tak, že i ty aplikace, které nyní nefungují, ani na specializovaných distribucích jako jsou Lindows, fungovat budou (jsou to především hry).

Útěk zdrojových textů Microsoftu, respektive Mainsoftu, byl v první řadě intelektuální krádeží. Tato krádež přináší mnoho nových rizik, ale také mnoho pozitiv, obojí v globálním měřítku. Zdrojáky OS Windows jsou na veřejnosti velikým pozitivem, stejně tak jako nebezpečnou zbraní. Záleží jen na tom, jakým způsobem se jich využije. 4 0182/FEL ❑



▲ **Stránky Mainsoftu byly přetíženy, po tom co se proslechlo, že odtud unikly kódy OS Windows NT4 a 2000.**



▲ **Představitelé Mainsoftu se k celé věci hodlají vyjádřit, až bude známo více informací.**