Aktivace produktu: Děravá ochrana Visty

Kdo instaluje Vistu, musí prokázat, že ji regulérně zakoupil. Vzdor aktivační povinnosti je však v oběhu mnoho pirátských kopií – a nejen v Asii. Microsoft už ale hackerský náskok dotahuje.

Valentin Pletzer, autor@chip.cz

Nelegální kopie softwaru jsou Microsoftu samozřejmě trnem v oku – především pak rozbujelé produktové pirátství v Rusku a v Číně. Podíl legálně získaných licencí je v těchto zemích podle šetření Microsoftu menší než 10 %; tyto odhady potvrzují i jiné zdroje. Nejdůležitější čínský velkoobchod (tržní podíl 90 %) udává, že v prvních dvou týdnech po zveřejnění Visty prodal jen 244 licencí. Pro srovnání – celosvětově bylo za první čtyři týdny realizováno kolem 20 milionů licencí.

XP: První pokusy o ochranu Windows

Především ve snaze omezit prodej zfalšovaných DVD s Windows začal Microsoft už u verze XP zostřovat její ochranu proti kopírování. Pirátským kopiím Windows má zabránit tzv. aktivace produktu (WPA), při níž uživatel svou kopii jakoby „přihlásí" u Microsoftu. Za tím účelem instalační program prozkoumá hardware počítače, shromáždí systémové informace o počítači a pak je společně se sériovým číslem Windows pošle Microsoftu. Seznam požadovaných informací vidíte v rámečku.

Microsoft pak z informací o počítači a ze sériového čísla vygeneruje kontrolní součet. Pokud je operační systém později instalován znovu, koncern pak na základě sériového čísla a nově zjištěných hardwarových informací dokáže poznat, zda se jedná o jiný počítač – a tím o porušení licenčních podmínek.

Softwarovým pirátům se však podařilo tuto protikopírovací ochranu prolomit. A Microsoft přitvrdil. „Zkoušku pravosti" (WGA = Windows Genuine Advantage) musí teď uživatel podstoupit nejen při instalaci Windows XP, ale i při každé větší aktualizaci. Podobně jako při původní aktivaci produktu koncern vyžaduje předání jednoznačných údajů. Microsoft přitom porovnává kontrolní součet z aktivace a aktuální systémové informace.

Avšak to, co zpočátku vypadalo jako úspěšná taktika, celý problém jen posunulo. Důsledkem totiž bylo, že piráti updaty buď ignorovali, nebo aktuálně dostupné aktualizace integrovali do instalačních DVD. Hlavním problémem přitom je, že má-li být operační systém bezpečný, musíte Windows při každé aktualizaci nově instalovat. Kdo na tuto hru nepřistoupí, stane se dříve či později obětí spywaru, který neopravené bezpečnostní mezery využívá.

Co všechno chce Microsoft vědět

- BIOS-Checksumme
- Kontrolní součet BIOS
- MAC adresu
- Sériové číslo pevného disku
- Jazykovou verzi operačního systému
- Verzi operačního systému
- Informace o PC a BIOS (Make, Version, Date)
- Výrobce PC
- Lokální nastavení uživatele
- Validační a instalační výsledky
- Produktový identifikátor Windows

Vista: Zlepšení ochrany

Ačkoliv už WGA představuje poměrně značnou překážku, u Visty Microsoft zkoušku pravosti ještě dále zostřil. Další přezkoušení WGA teď vyžaduje nejen v případech, kdy si uživatel chce něco od Microsoftu stáhnout, ale také nejpozději každých 180 dní. Cílem tohoto opatření je vyřadit z provozu zejména neopravené pirátské kopie.

Aby se to podařilo, opět se, jako u XP, předává Microsoftu celá řada informací. Jsou to údaje, které koncernu umožňují jednoznačnou identifikaci počítače. Proběhne-li tato kontrola úspěšně, Microsoft podle vlastního tvrzení shromážděná data ihned vymaže. Pokud však počítač kontrolou WGA neprojde, softwarový monarcha si zaznamená identifikaci a klíč produktu. Co se děje pak, o tom Microsoft mlčí. Přinejmenším teoreticky by se na základě IP adresy dal uživatel vyhledat – za předpokladu, že by spolupracoval provider.

Firmám jako Dell, HP nebo Sony nabízí Microsoft tzv. System Locked Preinstallation (SLP). Zde se při instalaci používá sériové číslo OEM a pro aktivaci neslouží kompletní informace o hardwaru, nýbrž jenom určitý údaj v BIOS (viz schéma).

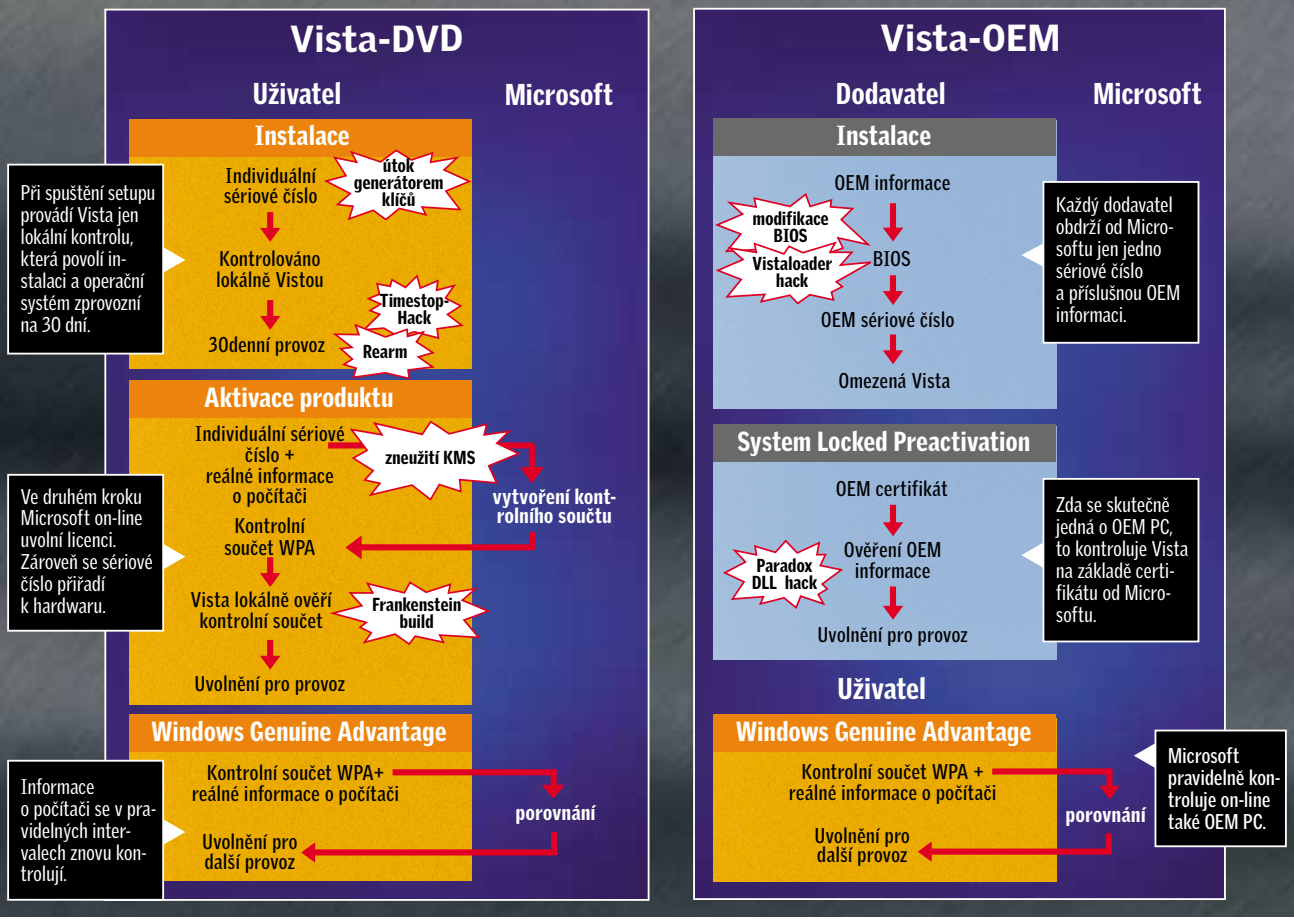
Útok: Hackeři překonají i ochranu Visty

Už před oficiálním zahájením prodeje letos v lednu kolovaly na internetu první kopie Windows Vista. K jejich zprovoznění však bylo zapotřebí několik komplikovaných zásahů, a výsledek proto piráty neuspokojil. Dokonce se zdálo, že jim už Microsoft „zatnul tipec". Avšak hackeři se nevzdali a své metody dále zdokonalovali. Připravili jsme pro vás malou chronologii hackerských napadení Visty:

Frankenstein build byl prvním útokem na protikopírovací ochranu Visty, který se objevil ještě během její „beta fáze". Poněvadž tou dobou v ní ještě byly implementovány jenom postupy WPA a WGA podobné verzi v XP, nebylo pro útočníky těžké ochranu prolomit. Když pak byla k dispozici finální verze a v ní daleko komplikovanější protikopírovací mechanismy, piráti využili prolomenou ochranu z beta verze a integrovali ji do Visty. Zdálo se, že tím na Microsoft vyzráli. Jenže varianty Visty obsahující tyto soubory se při vyhledávání aktualizací identifikují jako beta – a od 30. května už tato verze není aktualizována. →

Jak funguje aktivace produktu ve Vistě

Kvůli ochraně proti pirátskému kopírování kontroluje Vista licenční oprávnění na třech úrovních: sériové číslo, WPA a WGA. Přesto se hackerům podařilo najít body napadení jak u instalačních DVD, tak i u OEM verzí (vysvětlení útoků viz text).



→ **Timestop hack** přišel jako druhý. Jeho myšlenka byla prostá: 30denní lhůtu pro aktivaci jednoduše protáhnout do nekonečna. V zásadě to také tak funguje – až na to, že tuto verzi nelze aktualizovat. A bez bezpečnostních aktualizací se takovýto systém nedá rozumně použít.

Rearm je vlastně jen oficiálně použitelný příkaz, který ve Vistě umožňuje 30denní lhůtu i několikrát prodloužit. S tím je ovšem definitivně konec po 120 dnech. Pak už Windows žádné další prodlužování nepřipustí – přestože podobná pověst mezi uživateli ještě stále obíhá.

Zneužití KMS serveru (Key Management Service) se poprvé objevilo jako čínská pirátská kopie. K podvodu využívá „Volume Activation 2.0" pro Vista Business a Enterprise. Aby totiž ve velkých podnicích kvůli aktivaci nemusely s centrálou komunikovat všechny počítače, Microsoft takovým firmám nabízí speciální serverový software, který pracuje jako aktivační proxy. Stačí pak jednou aktivovat KMS, a ten už zprovozní všechny počítače v místní síti. Lze tak ovšem aktivovat jen provedení Vista Enterprise a Business. Kromě toho, pokud Microsoft odepře KMS serveru aktivaci, jak se to už u pirátských kopií stalo, neprojdou už kontrolou WGA ani klienti.

Generátory klíčů se samozřejmě vyrojily i pro Vistu. Jejich koncepce využívá „hrubou sílu": malá aplikace má generovat různá registrační čísla tak dlouho, dokud nenajde platný klíč. Tento útok má však hned dvě slabiny: za prvé trvá vyzkoušení klíče relativně dlouho, za druhé musí být nalezený klíč akceptován nejen lokálně, nýbrž také on-line u Microsoftu. A počet klíčů v jeho databance je podstatně menší než počet klíčů, které Vista akceptuje na počítači.

Modifikace OEM BIOS dosud Microsoft ignoruje. Poněvadž změny v BIOS nejsou pro uživatele bez rizika, prozatím si s nimi v Redmondu starosti nedělají. „Není naším cílem bránit v činnosti kdejakému šílenému vědci, který si usmyslel cracknout Windows," říká k tomu mluvčí koncernu.

Paradox je skupina hackerů, jejíž produkt Microsoftu rozhodně nebyl vhod: ovladač, který se nainstaluje pod Vistou, zachycuje požadavky na BIOS a simuluje pak pravý OEM BIOS – aniž by vůbec musel přistupovat k hardwaru. Dnes už je však ovladač od Paradoxu rozpoznáván, a tato metoda je tedy nepoužitelná.

Vistaloader je bootovací zaváděč, který funguje podobně jako ovladač Paradox. Speciální bootovací správce prostě emuluje celý BIOS, který hackeři zkopírovali z nějakého OEM počítače. I v tomto případě je však jen otázkou času, kdy bude Microsoft schopen tento software rozpoznat a deaktivovat.