KÉMEK A FILMEN, KÉMEK A GÉPBEN

A digitális jogkezelés vadhajtásai

Sorozatunk harmadik epizódjában a Mr. és Mrs. Smith című film elhíresült német kiadása kapcsán a digitális jogkezelés (Digital Right Management – DRM) helytelen felhasználásáról lesz szó.

A rootkites rejtőzködő technikát a szerzői jogok őrzői is igyekeznek kiaknázni. Jó-e ez nekünk, és ha nem, hogyan védekezhetünk ellene? Mint tudatos vásárlók, ebben a témában igyekszünk most hasznos információkkal szolgálni.

Ahova nézek, ott rootkit terem

Múlt havi cikkünkben már részletesen beszámoltunk arról, hogy 2005 novemberében a Sony BMG zenei CD-ken lévő másolásvédelmi rootkit milyen nagy vihart kavart. Érdekes módon a Sony baklövése után mások mégis újra megpróbálkoztak rootkitekkel felvértezett másolásvédelemmel. 2006 februárjában a Mr. és Mrs. Smith című mozifilm német nyelvű DVD-kiadásán találtak hasonló kártevőt. Az F-Secure beszámolója szerint az egyik német internetes magazin, a **www.heise.de** szerkesztői figyeltek fel arra, hogy a Mr. és Mrs. Smith DVD számítógépbe helyezésekor egy telepítőprogram indult el. Ez nem más volt, mint a Settec Alpha másolásvédelmi szoftver, a meglepő azonban az, hogy rootkit technikákat használva rejtette el magát a felhasználó elől.

Definíciója szerint a rootkit egy olyan szoftver, mely képes elrejteni magát mind a felhasználók, mind a különféle biztonságtechnikai termékek elől. Ezt különféleképpen teheti meg: van, amelyik egy könyvtárlistázás során a hozzá tartozó fájlokat nem mutatja meg, míg igen elterjedt az a módszer is, hogy a futó alkalmazások listáján nem jelenik meg az éppen aktív rootkit munkafolyamatainak neve. Ha nem fogadjuk el a DVD végfelhasználói licencszerződését (EULA, End User License Agreement), a számítógép egyszerűen kiadja a DVD-t, ha elfogadjuk, akkor viszont telepíti a jogvédő programot a gépre.

Alpha Kémbázis

A szóban forgó Settec Alpha rootkit a Sony programjánál talán kevésbé veszélyes, mert nem rejt el mást, csak saját programállományát, ettől függetlenül mégis biztonsági kockázatot jelenthet, és akár azt is elősegítheti, hogy hackerek vagy vírusok hatoljanak be a gépbe. A NOD32 képes felismerni és eltávolítani e kellemetlen alkalmazást, de magának a DVD-nek a kiadója is megjelentetett egy eltávolító szoftvert, amelyre azért volt szükség, mert alapesetben a programot nem lehet sem a Start menüből, sem pedig a Vezérlőpult segítségével eltávolítani. Kizárólag netes kapcsolattal lehet uninstallálni, több lépés és szándékmegerősítés után, internetkapcsolat híján viszont sajnos nem lehet tőle megszabadulni.

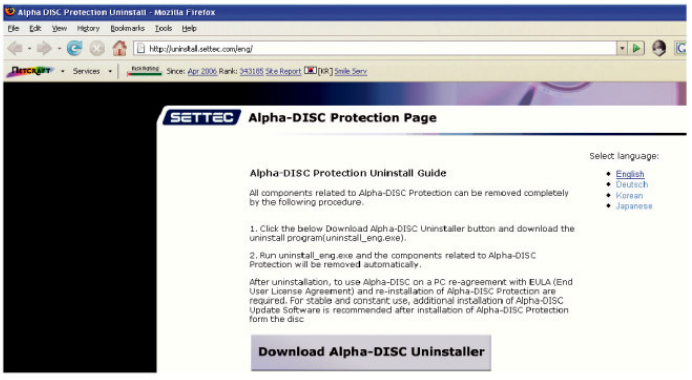
Az első hírek szerint a fertőző DVD német és finn nyelvterületen került a boltokba, de a megerősített információk szerint csak és kizárólag a német változat tartalmazta a rootkitet, a finn verzió nem. (Aki hozzá akar jutni, nincs más dolga, mint rákeresni a németországi eBay portálon, a mai napig keringenek belőle példányok.)

Itt és minden más automatikusan induló lemez esetében érdemes megtanulnunk, hogy a Windows automatikus AutoRun funkcióját (és ezzel bármely kártékony program települését) a lemez behelyezésekor a <Shift> billentyű 10 másodperces lenyomásával hatástalaníthatjuk. Az újabb rootkitbotrány kipattanása után ezt a módszert a Mr. és Mrs. Smith DVD csomagolásán egy piros matrica fel is tüntették. A DVD-re került másolásvédelmi rootkit csak Windows alatt települ, asztali lejátszókkal vagy más operációs rendszer alatt semmilyen problémát nem okoz, a film lejátszását sem akadályozza. Az Alpha-DVD rootkitet készítő Settec cég korábban a dél-korai LG vállalatnak dolgozott.

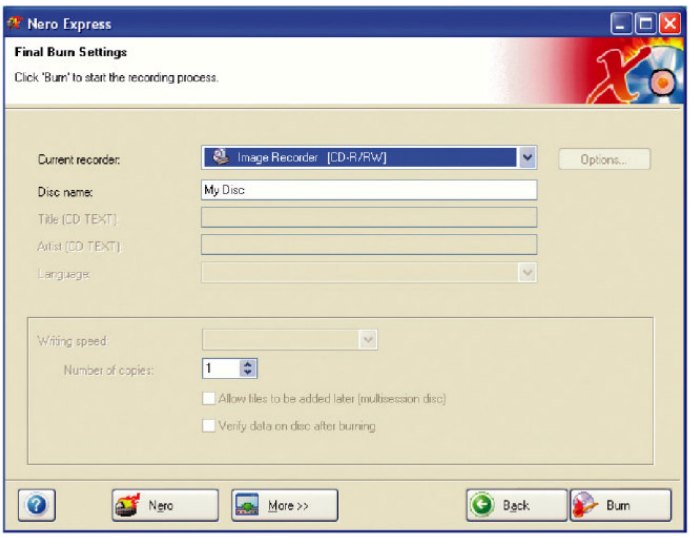
Úgy tűnik, a harc nem kizárólag a képernyőn zajlik: a Nagy Testvér helyett sok Kis Testvér kíváncsi tekintete igyekszik mind jobban kifürkészni hétköznapi életünket, ellenőrzést gyakorolni és titokban információkat szerezni

DRM, mert megérdemlem

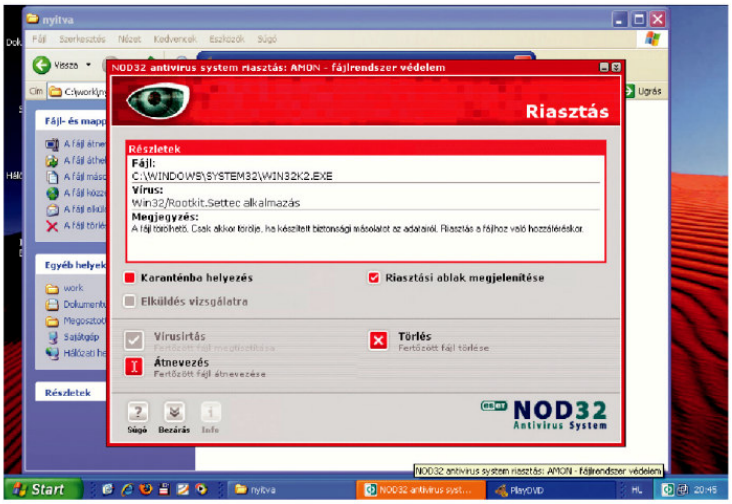
A digitális anyagok szerzői jogvédelme az a módszer, mellyel a kiadók és a szerzői jog tulajdonosai kezelni akarják, továbbá ellenőrzésük alatt akarják tartani a tőlük származó adatok – többnyire médiafájlok vagy akár dokumentumok – mozgását a különböző lejátszó eszközökön, illetve a számítógépek között. A kellő szakmai gonddal kidolgozott DRM-rendszerek nem rejtenek veszélyt magukban, igaz, így is boszszantóan korlátozzák a felhasználók lehetőségeit. Mi most a kifejezetten alattomos és nem kellőképpen tesztelt, ezért rendszerünk stabilitását veszélyeztető megoldásokra hív-



Amikor kitör egy újabb rootkitbotrány, a gyártók kénytelen-kelletlen közreadják az eltávolító eszközt. A nagy kérdés persze ezek után az, hogy az események tükrében a koreai weboldalról letölthető újabb programban vajon megbízhatunk-e?



Ha települt a másolásvédelem, gyakran búcsút inthetünk a CD/DVD-írásnak, mert meghajtóink egyszerűen eltűnnek a kiválasztható eszközök listájáról



A NOD32 2.7 vírusirtó program – ha az állandó védelemben bekapcsoljuk a Veszélyes alkalmazások keresése opciót – már a Settec Alpha telepítési kísérletnél védelmet nyújt

juk fel a figyelmet – sajnos van belőlük jócskán.

A Sony a First 4 Internet cég XCP (Extended Copy Protection) másolásvédelmi megoldását választotta, hogy néhány CD-n kiadott zenei anyaga használatát ellenőrizhesse. Az XCP-vel védett lemezeknél korlátozták a készíthető CD- vagy DVD-másolatok számát, valamint azt is ellenőrizték, hogy alkalmaztak-e rippelést (a CD-audioanyag lemásolása és számítógépes formába – WAV, MP3 stb. – való átalakítása) az adott zenei anyagnál, számítógépen vagy más hordozható zenelejátszó esetében. Ezek a zenei CD-k a számítógépen mindaddig nem voltak lejátszhatók, míg nem telepítették a mellékelt szoftvert. A korlátozó funkciók mellett az XCP fájlokat és futó folyamatokat rejtett el, Registry-kulcsokat és -bejegyzéseket módosított, manipulálva ezzel az operációs rendszer alapértelmezett API-függvénykészletének végrehajtását. Bár maga a program önmagában nem jelentett veszélyt – mint azt a múlt hónapban taglaltuk – de lehetőséget adott a különféle veszélyes kártevőknek elrejtőzni mögéje a biztonsági szoftverek elől.

Nem feltétlenül szükséges rootkit ahhoz, hogy egy DRM-rendszer veszélyes legyen! Egyes DRM-megoldások adott esetben kárt is tehetnek a számítógépben vagy más készülékekben. Vannak olyanok, amelyek inkompatibilisek lehetnek a számítógép beállításaival, ezzel a rendszer összeomlását okozhatják. A biztonság akkor is kockán forog, ha a DRM-rendszer ügyetlen kiegészítő programokat telepít a számítógépre. Ezek aztán konfliktusba kerülhetnek a DVD-meghajtóval, DVD-, illetve egyéb médialejátszó programunkkal vagy más, többnyire multimédiás funkcióival. Pontosan ez következett be a Mr. és Mrs. Smith DVD esetében. Több fórumra is érkezett olyan felhasználói panasz, hogy a program telepítése után a DVD-írók és virtuális meghajtók elérhetetlenek lettek, a **heise.de** gépein a program jelenlétében bármilyen DVD-adatlemez hibásan lett megírva. Egy ilyen gépen hiába indítjuk el a CD/DVD-író programot (például Nero, Alcohol), az optikai egységeket nem tudjuk kiválasztani az egységek legördülő menüjében. Az a szomorú, hogy ebben az esetben a DRM csak azt leckéztette meg, aki boltban, pénzért megvásárolta, és legálisan birtokolta a korongot.

A norvég Jon Johansen (DVD Jon) először a DVD-k másolásvédelmének feltörésével vált híressé. Amikor 2003-ban nyilvánosságra hozta az iTunes Music Store másolásvédelmének feltörésére írt programját, egy újabb per várt rá. A perek alatt tömegek tüntettek mellette, az első per alapjául szolgáló DVD-törő kódot pedig még pólókra is rányomtatták

Mire figyeljünk?

Akár online, akár fizikai formában keresünk zenei, illetve videoanyagot, az esetleges vásárlás előtt alaposan tanulmányozzuk át a csomagoláson vagy a terméklefíráson található jelöléseket. A Copy Protected, illetve Copy Control feliratok egyértelműen jelzik az esetleges másolásvédelmet. Ha online vásárolunk, ne kattintsunk automatikusan a Next gombra, hanem figyelmesen olvassuk el a licencszerződést. Legjobb, ha kinyomtatjuk, és ha kétségeink vannak, kérjünk fordítási, illetve értelmezési segítséget. Online letölthető tartalom esetén tájékozódjunk annak tárolási, másolatkészítési lehetőségei felől, illetve arról, hogy a különféle adathordozóra (MP3-lejátszó, CD/DVD) való másolása nem ütközik-e akadályba.

Ha az adott feltételek nem megfelelőek számunkra, álljunk el a vásárlástól. Ha pedig később úgy érezzük, hogy a hiányos tájékoztatás vagy más ok miatt hátrány vagy kár ért bennünket, forduljunk a Fogyasztóvédelmi Felügyelethez.

Végjáték, végkövetkeztetésekkel

Annak idején a Sony nem kezelte megfelelően az esetet a nyilvánosság előtt, és első javítási kísérlete is alkalmatlannak bizonyult. Ez egy olyan segédprogram volt, amelyet csak az vehetett igénybe, aki előtte kitöltött egy űrlapot. Használatával el lehetett ugyan távolítani a védelmi programot, ettől kezdve viszont nem lehetett lejátszani a számítógépen a megvásárolt zenei CD-t – vagy kikapcsolhattuk a védelmi program rejtettségét. Jelentések szerint ez a kezdeti javítócsomag nagyméretű volt és alig tesztelt, sőt egy illegális jelentést küldő funkcióval is rendelkezett („hazatelefonált"), amelyről persze egy árva szó sem esett a végfelhasználói licencszerződésben.

Hosszú pereskedés után a Massachusetts állam főügyésze által közzétett bejelentés szerint 2006 karácsonya előtt sikerült megállapodni a Sony BMG-vel a rootkitbotrány rendezéséről, amelynek eredményeként jelentős kártérítést fizettek ki mind az Egyesült Államoknak, mind a vásárlóknak. A megállapodás értelmében a pert indító 39 államból álló csoportosulás összesen 4,25 millió dollárt kapott, a pórul járt vásárlók pedig a korábbi egyezményekben rögzítettekhez hasonlóan a Sony BMG weboldalán jelezhették igényüket, melynek elfogadása esetén egyenként 175 dollárt kaptak kézhez. Ez a cég véleménye szerint megfelelő összeg a rootkittel fertőzött zenei albumokért cserébe. Ezzel a Sony végre maga mögött hagyhatta ezt a kellemetlen időszakot, hiszen a perek legnagyobb részét így lezárták.

A mi szempontunkból az a fontos momentum, hogy ebben az egyezményben kikötötték: a kiadó a jövőben nem használhat az XCP-hez hasonló DRM másolásvédelmi megoldást.

Osztjuk azt a nézetet, hogy a különböző fejlesztőcégeknek (és nem csak a másolásvédelmi eszközöknek) távol kellene tartani magukat mindenféle rejtett machinációktól. Az ilyen módszerek biztosan nem szolgálják a felhasználó érdekeit, és sok esetben akár újabb biztonsági sebezhetőségek kialakulásához vezethet. Ezek után csak reménykedhetünk, hogy két ilyen súlyos eset kapcsán a forgalmazók a jövőben talán átgondoltabb, és ránk, vásárlókra nézve kedvezőbb megoldásokkal rukkolnak elő. Sajnos várhatóan a DRM nélkülözhetetlen kelléke lesz a jövő digitális termékeinek, de mi már annak is örülnénk, ha ez valóban csak az adott tartalmat védené, és másban nem akadályozna vagy szolgáltatna ki minket, valamint nem kémkedne utánunk.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk **(velemeny@pcworld.hu).**

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Híradások a Mr. & Mrs. Smith DVD esetről:
hopp.pcworld.hu/3716, hopp.pcworld.hu/3717, hopp.pcworld.hu/3718

Használati útmutató a digitális jogkezeléshez, magyarul:
hopp.pcworld.hu/3715

A hivatalos Settec Alpha-DVD rootkit-eltávolító:
uninstall.settec.com/eng/

A digitális másolásvédelem jelölései:
ukcdr.org/issues/cd/warnings/