

## Artikel Hoe hackers via USB-sticks het netwerk overnemen

Door [Redactie](#) op maandag 24 december 2007 11:08

Regelmatig verschijnen er onderzoeken waarbij uitgedeelde of gevonden USB-sticks zonder enige schroom door het personeel op hun werkcomputer worden aangesloten, maar volgens Microsoft MVP Jesper Johansson wordt deze tactiek echt toegepast door criminelen om bedrijfsnetwerken te infiltreren. Via eenvoudig te verkrijgen tools zoals [Hacksaw](#) en [Switchblade](#) is het kinderspel voor een aanvaller om wachtwoorden, documenten en andere vertrouwelijke systeemgegevens naar zich toe te laten mailen of binnen 45 seconden op de USB-stick te zetten. Een aanvaller hoeft dan ook maar even fysiek toegang tot een machine te hebben om alle gegevens op te slurpen.

Windows Vista beschikt over enkele maatregelen om misbruik door USB-sticks tegen te gaan. Zo kan een systeembeheerder bijvoorbeeld autoplay of het aansluiten van dit soort informatiedragers blokkeren. Ondanks deze maatregelen blijft het belangrijk dat kantoorwerkers met verminderde rechten werken. "Als de gebruiker een standaard gebruiker is, kan een exploit beperkte schade aanrichten. Het kan nog steeds gebruikersgegevens en andere informatie stelen. De aanval zal waarschijnlijk geen impact op het bedrijfsnetwerk hebben", [aldus](#) Johansson

*UBM Global: Gebruik DriveLock Basic in combinatie met DriveLock Applicatie Launch Filter*

### DriveLock Basic

*Blokkeert computer toegang voor verwijderbare opslagmedia (alles met een driveletter) dynamisch en configureerbaar*

- *USB memory stick*
- *Diskette, CD/DVD-ROM, externe harddisk, maar kan ook autorisaties verlenen voor gespecificeerde media, bijvoorbeeld een speciale Update CD-ROM*
- *Andere zoals Ipod, sommige digitale camera's, etc. mits door besturingssysteem herkent als drive; hangt af van de fabrikant*

*Toegang kan selectief worden toegestaan*

- *Voor gebruikers en / of groepen*
- *Alleen-lees of lees-schrijf bevoegdheden van en naar verwijderbare opslagmedia en randapparaten met een schijf*
- *Gebaseerd op fabrikant / product informatie en serienummer*
- *Gebaseerd op geheugencapaciteit van verwijderbare opslagmedia*
- *Gebaseerd op encryptie status, geforceerde encryptie*

*Automatisch toewijzen van voorgedefinieerde drive letters*

- *Aan alle drives zodra deze worden verbonden, bijvoorbeeld memory sticks*

*Autorisaties zijn mogelijk voor nagenoeg alle mobiele opslagmedia zoals in het overzicht van de Home pagina getoond, in aanvulling daarop in het bijzonder nog*

- *Card-readers (CF, Microdrive, MagicStore, SM, MMC/RS-MMC, SD/Mini-SD, xD)*

- *U3-stick, biometrische randapparaten*
- *Blackberry, Windows Mobile Handhelds*

#### *Content (file) filter*

- *Filtert ongeautoriseerde bestand extensies of file typen, en de inhoud van de bestanden*
- *File typen kunnen definiëren als onderdeel van de policy*
- *Additionele opties geven de mogelijkheid om uitzonderingssituaties en – gebruikers te configureren zodat virus scanners in staat zijn de scans sneller uit te voeren*
- *Filtert inkomende en uitgaande bestanden*
- *White lists kunnen worden gebaseerd op een combinatie van file filters en specifieke gebruikers*

#### *DriveLock Applicatie Launch Filter*

- *Autoriseren en controleren van applicaties*
  - *Op client PC's*
  - *Binnen Terminal Services client sessies*
  - *Die actief zijn in het netwerk*
  - *Ter bescherming tegen aanvallen, inclusief zero-day attacks, waarvoor nog geen patches verkrijgbaar zijn*
- *Keuze uit operationele modes*
  - » *Whitelist mode: alleen specifieke applicaties zijn toegestaan*
  - » *Blacklist mode: specifieke applicaties worden geblokkeerd*
  - » *Scan mode: opstarten van applicaties wordt gelogd zonder toepassingsregels*
  - » *Test mode: regelverwerking is gelogd zonder blokkering van applicaties*
- *Templates kunnen worden gecreëerd van huidige lopende applicaties*
- *Blacklist en whitelist regels kunnen worden gecombineerd om uitzonderingen te creëren*
- *Werkingsprincipe*
  - » *Onderschept elke start van een applicatie*
  - » *Verwerkt een hash van de executable*
  - » *Vergelijkt deze hash met alle beschikbare whitelist en blacklist regels*