

Hacker verstopt Trojaans paard in firmware MP3-speler

Door Redactie security.nl op vrijdag 23 november 2007 13:45

Een beveiligingsonderzoeker heeft een nieuwe manier gevonden om via MP3-spelers systemen te infecteren. Het was al langer bekend om malware via de Autorun optie te verspreiden of via een gehackte flash chip een buffer overflow op het systeem te veroorzaken. Nu is het een hacker gelukt om de firmware van een MP3-speler aan te passen. Zo kan men niet alleen .exe bestanden infecteren, maar ook kwetsbaarheden in multi media bestanden misbruiken. "De payload kan een zichzelf verspreidende Trojan, keylogger of alles zijn wat je maar kunt verzinnen." De enige restrictie is de hoeveelheid geheugen die in de firmware beschikbaar is.

Een andere optie, als het injecteren van bestanden niet mogelijk is, is het mogelijk om autorun bestanden te schrijven, die zodra de speler op een PC wordt aangesloten, bepaalde commando's uitvoert. De aanval is verder onzichtbaar voor de gebruiker en zelfs voor experts is het lastig om de aanval te traceren naar de firmware van de MP3-speler. Een aanvaller zou het geprepareerde apparaat bijvoorbeeld kunnen uitdelen of bewust ergens achterlaten, in de hoop dat iemand het meeneemt een aansluit. In het verleden zijn er al meerdere tests geweest waarbij kantoorpersoneel een CD of USB-stick cadeau kreeg, en de meesten die gewoon via hun kantoor PC openden.

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*