

Artikel Malware steeds vaker via USB-sticks

Computable 23 november 2007

Een van de belangrijkste eigenschappen die een virus of andere vorm van malware nodig heeft, is de mogelijkheid zich te verspreiden. E-mail is daar de afgelopen jaren de perfecte drager voor gebleken.

Verstoort wist de malware zich soms razendsnel over de wereldbol te verspreiden. In de wedrace tussen virusmakers en leveranciers van antivirussoftware zijn de laatste een flink eind gekomen. Hoewel er tegen een gepersonaliseerde criminele aanval nog steeds weinig is te doen, heeft een groot gedeelte van de internetgebruikers goede antivirusmaatregelen genomen. Ontwerpers van malware zitten nooit stil, meent Roel Schouwenberg, senior virus researcher van [Kaspersky Lab](#) Benelux.

"De wedloop gaat altijd door en nu we mail en webapplicaties steeds beter onder controle krijgen, gaat men op zoek naar alternatieven om malware te verspreiden. Daarbij hebben ze goed naar het verleden gekeken. In de begintijd van de personal computer werden virussen vooral verspreid via floppydisks. Wanneer tekst en andere data van de ene pc naar de andere moest, werd door de virussoftware een onzichtbaar bestand meegestuurd dat de ontvangende pc besmette. Zo kon een virus zich langzaam verspreiden, al was het besmettingsgebied vaak relatief klein."

Bij de bron

Volgens Schouwenberg grijpt men weer terug naar deze analoge manier van verspreiden. "De usb-sticks zijn de floppies van vandaag. We zien in toenemende mate malware ontstaan die zich juist richt op deze manier van verspreiden. Daarbij gaat het overigens niet alleen om gebruikers die onvoorzichtig zijn. Wat we in de afgelopen maanden hebben gezien, is dat criminelen vaker proberen dicht bij de bron te komen en de pc's besmetten die verantwoordelijk zijn voor het formatteren van de gegevensdragers."

Het zijn niet alleen usb-sticks die op deze manier worden voorzien van malware. In september raakten in de Chinese fabriek van hardeschijvenfabrikant [Maxtor](#) circa tweeduizend harde schijven besmet met het AutoRunAH-virus dat wachtwoorden steelt en verbinding maakt met dubieuze websites.

Games

Schouwenberg: "Bij deze besmettingen zien we ook een toename van virussen die wachtwoorden van online games stelen. Karakters in deze spellen zijn geld waard geworden. Op eBay zie je dat er al forse bedragen worden geboden voor gewilde figuren. We hebben het laatst met Habbo-hotel gezien. Met virtuele zaken is inmiddels grof geld te verdienen en dat zien criminelen ook."

UBM Global: Gebruik DriveLock Basic in combinatie met DriveLock Applicatie Launch Filter en voorkom daarmee het opstarten van niet geautoriseerde applicaties

[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*