

## Mysterieus internetvirus kan hele landen offline halen

Van onze verslaggever Bard van de Weijer  
gepubliceerd op 19 maart 2009 17:26, bijgewerkt op 19 maart 2009 18:04

AMSTERDAM - Een mysterieus virus dat al maanden over het internet waart, is inmiddels zo wijdverbreid en geavanceerd dat het door de makers gebruikt kan worden om complete landen offline te halen. Het is zelfs mogelijk dat het internet ontregeld raakt. Dat stellen computerwetenschappers van het Amerikaanse SRI International.

Wie er achter Conficker of Downadup, zoals de kwaadaardige software genoemd wordt, zitten, weet niemand. Evenmin is duidelijk waar het virus vandaan komt. Zelfs de bedoeling van Conficker is onbekend. Het virus verspreidt zich en past zich telkens aan om antivirussoftware te omzeilen, maar verder doet het niets.

Volgens schattingen van de Finse virusbestrijder [F-Secure](#) waren in februari wereldwijd acht miljoen computers besmet. SRI gaat uit van een lager aantal, maar stelt dat het gaat om de grootste besmetting sinds 2004, toen het Sasser-virus miljoenen pc's ontregelde.

### Instructies

Experts denken dat Conficker wacht op instructies van de onbekende makers. Deze instructies zullen verlopen via een van de 50 duizend domeinnamen die de nieuwste versie van Conficker dagelijks 'bedenkt'. Als de makers een van die domeinnamen activeren, zal het virus van deze site instructies downloaden voor een volgende stap.

Dat kan van alles zijn, zei onderzoeker Phillip Porras van SRI International tegen [The New York Times](#). 'Het meest beangstigende aspect van Conficker is zijn potentiële mogelijkheden schade aan te richten.' In het beste geval, zegt Porras, wordt het gebruikt voor massale internetfraude. In het slechtste wordt Conficker ingezet voor elektronische oorlogsvoering en kunnen complete landen worden ontregeld.

Patrik Runald van F-Secure acht de kans niet groot dat een overheid achter het virus zit. 'Maar uit te sluiten is het niet', zegt Runald.

### Reageren

Het lijkt erop dat de makers reageren op wat virusbestrijders bekend maken over Conficker. Aanvankelijk genereerde het virus dagelijks slechts 250 domeinnamen, maar toen enkele antivirusconcerns het algoritme kraakten, waardoor deze domeinnamen geblokkeerd konden worden, pasten de makers het virus aan.

Op 1 april verschijnt de derde versie van Conficker, dat vanaf dat moment dagelijks 50 duizend namen 'bedenkt', ontdekte de Amerikaanse virusbestrijder CA. Daardoor wordt het voor virusbestrijders een stuk lastiger deze domeinnamen te blokkeren.

Er zijn aanwijzingen dat het virus afkomstig is uit de Oekraïne. In de eerste versie zat

een code die computers met IP-adressen uit dit land vrijwaarden van besmetting. In latere versies is deze 'vrijstelling' verdwenen.

### **Lek**

Het virus verspreidt zich via een lek in het besturingssysteem Windows van Microsoft. Dat lek is al in oktober gedicht, maar doordat niet elke gebruiker zijn systeem updatet, kan Conficker zich toch verspreiden. Eenmaal geïnstalleerd laat Conficker zich lastig verwijderen, onder meer doordat het de toegang blokkeert tot antivirussites. Ook voorkomt het dat Windows een pleisterprogramma installeert. Doordat het virus zich vooralsnog slapende houdt, merken veel gebruikers niet dat ze zijn geïnfecteerd.

Microsoft heeft onlangs een beloning uitgelooft van 250 duizend dollar aan degene die informatie verschaft die leidt naar de makers. Diverse bedrijven hebben inmiddels hulpmiddelen ontwikkeld om het virus van een pc te verwijderen, maar het is onduidelijk of die ook werken voor de versie die op 1 april actief wordt.

Het lijkt erop dat Conficker zich niet langer probeert te verspreiden, zeggen medewerkers van Symantec, maar dat het vooral probeert niet ontdekt te worden op machines waarin het zich genesteld heeft.

url: [http://www.volkskrant.nl/multimedia/article1166986.ece/Mysterieus\\_internetvirus\\_kan\\_hele\\_landen\\_offline\\_halen](http://www.volkskrant.nl/multimedia/article1166986.ece/Mysterieus_internetvirus_kan_hele_landen_offline_halen)