nrc.nl

# WannaCry werd mede mogelijk gemaakt door lek bij de NSA

*Liza van Lonkhuyzen 14 mei 2017 om 15:58*

5-7 minuten

---

De computers van Chinese universiteiten, Spaanse elektriciteits- en gasbedrijven, het Franse autobedrijf Renault en spoorwegvervoerder Deutsche Bahn raakten besmet. In het Verenigd Koninkrijk werden computers van ambulancebedrijven, ziekenhuizen en huisartsenpraktijken gegijzeld. Operaties werden afgeblazen en artsen konden niet meer bij medische dossiers.

Het afgelopen weekend werden tal van grote bedrijven en organisaties getroffen door de malafide software WannaCry – een vorm van *ransomware*. Dat is software die de bestanden van computers versleutelt en gebruikers om losgeld – enkele honderden euro's – vraagt om weer toegang tot de computer te krijgen. Parkeerbedrijf Q-Park was een van de weinige Nederlandse slachtoffers. Bij parkeergarages in steden als Rotterdam en Gouda konden mensen door de malware niet meer betalen.



Een Britse veiligheidsexpert, die een zogeheten 'kill switch' vond, wist het virus te beteugelen. In de code van de malware trof hij een lange naam aan van een denkbeeldige website. Deze

domeinnaam officieel registreren bleek het virus af te remmen.

Het gevaar is desondanks niet geweken. Zondag sprak Rob Wainwright, directeur van Europol, de vrees uit voor veel nieuwe infecties op maandag als veel kantoorcomputers weer worden opgestart.

## Gestolen van de NSA

Hoe lukte het de cybercriminelen om een dergelijke ‘succesvolle’ aanval uit te voeren? Criminelen gebruikten een kwetsbare plek in de software van Windows om de computers over te nemen. Deze ‘ingang’ komt volgens beveiligingsexperts rechtstreeks bij de NSA vandaan. Een hackercollectief genaamd ‘Shadow Brokers’ had het hackgereedschap van de Amerikaanse geheime dienst gestolen en vorige maand online gezet.

Dat roept een belangrijke vraag op: hoe gevaarlijk is het dat geheime diensten een arsenaal aan zwakke plekken in software gebruiken voor hun spionagedoeleinden? Privacy-activisten wijzen erop dat deze ellende was voorkomen als de NSA Windows waarschuwde over het lek vóór het in de gaten had dat z’n hackgereedschap was gestolen. Windows heeft het lek twee maanden geleden gedicht door een update uit te brengen, maar de getroffen organisaties hebben die update niet op tijd uitgevoerd.

## Wat kun je doen om je computer te beschermen tegen WannaCry?

De WannaCrypt-ransomware (bijnaam: WannaCry) kan alle versies van Windows infecteren die niet de MS-17-101-update hebben gehad. De computer updaten is dus het eerste en belangrijkste om te doen. Apple-gebruikers kunnen niet door de

malware WannaCrypt worden geïnfecteerd.

Pas daarnaast op met het openen van bestanden in e-mails, of het aanklikken van linkjes. Ransomware kan zich bijvoorbeeld verschuilen in een nepfactuur.

Het is altijd verstandig om regelmatig back-ups te maken van bestanden. Zo zijn ze veiliggesteld tijdens een ransomware-besmetting.

Voor geheime diensten als de NSA en de Nederlandse AIVD zijn voor de fabrikant onbekende kwetsbare plekken in software - zogeheten *zerodays* - een belangrijke manier om doelwitten te bespioneren. Officieel horen deze geheime diensten een belangenafweging te maken als ze zo'n zeroday vinden: is het veilig deze te gebruiken, of moet de fabrikant worden ingeseind? „Bij veelgebruikte systemen als Windows weegt het belang om het lek te laten dichten op tegen belang om ermee te spioneren", zegt Erik de Jong van beveiligingsbedrijf Fox-IT.

## Wapenwedloop

Overheden zijn al jaren bezig met een soort wapenwedloop in cyberspace. Hoogleraar cyberveiligheid Jan van den Berg zegt dat deze begon na de aanslagen van 11 september 2001. „Alle beurzen werden opengetrokken voor geheime diensten. De steeds geavanceerdere tools die zijn gebouwd, worden vroeg of laat ontdekt door contra-spionnen of criminelen."

„We herkennen bij computercriminelen spionagetrucjes die zijn afgekeken van geheime diensten," zegt De Jong. „Dat is niet vreemd: hoe goed je ook bent als aanvaller, er blijft een kans dat je spionagegereedschap wordt ontcijferd en hergebruikt."

Dat werd voor het eerst duidelijk bij het virus Stuxnet, dat in 2010 werd ontdekt. Vermoedelijk gebruikte de VS het om het Iraanse

nucleaire programma te saboteren. Trucs van het geavanceerde cyberwapen werden na de ontdekking hergebruikt door criminelen.

Door de Snowden-onthullingen weten we dat dat de NSA een afdeling heeft waar hacks worden gefabriceerd en zwakke plekken in software worden gezocht of gebouwd. Bekend is dat overheden en geheime diensten deze zerodays ook aanschaffen van commerciële bedrijven met hackers in dienst, en dat daar grof geld aan wordt verdiend. Een zeroday voor een veelgebruikt systeem dat bekendstaat als veilig, kan vele honderdduizenden euro's opleveren.

In Nederland mogen, als een nieuwe wet computercriminaliteit door de Eerste Kamer gaat, naast inlichtingendiensten ook politie en justitie verdachten hacken met deze zerodays. „Overheden stimuleren de markt voor zerodays, in plaats van dat gaten worden gedicht", zegt Kees Verhoeven, Tweede Kamerlid van D66. „Uiteindelijk zorgt dit voor meer onveiligheid."