# Computercriminelen krijgen vrij spel door gigantisch beveiligingslek

Computergebruikers met een Windows-pc zijn meer dan ooit kwetsbaar voor een hacker-aanval of virus. Onlangs werd er een beveiligingslek ontdekt waarmee de computer op honderden plaatsen tegelijk openstaat, en waarlangs de inbreker zich de volledige controle over de pc kan verschaffen. De eerste aanvallen zijn ondertussen al gemeld.

DOOR RONALD MEEUS

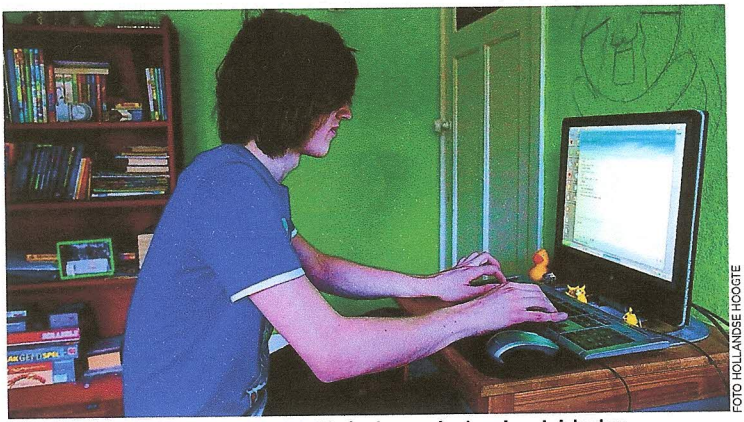

FOTO HOLLANDSE HOOGTE

■ Via populaire software als iTunes en Firefox kunnen hackers in pc's inbreken.

# Windows open voor hackers

**BRUSSEL ● Beveiligingsexperts ontdekten dat er één punt is waarlangs booswichten zich de toegang kunnen verschaffen tot enkele honderden Windowsprogramma's. Bovendien is het gat erg moeilijk te dichten.**

Microsoft sloeg afgelopen maandag zelf alarm over het beveiligingsprobleem, waarmee driehonderd tot vierhonderd programma's onder zijn Windowsbesturingssysteem kunnen worden gehackt. Daar zit vaak gebruikte software tussen, zoals iTunes, Firefox, en ook een paar van Microsofts eigen programma's, zoals PowerPoint en mailprogramma Windows Live Mail. Kern van het probleem: al die programma's hebben dezelfde fout, en leveren daarlangs dus tegelijkertijd toegang tot de computer. "Stel dat je op het internet per ongeluk een malafide PowerPointbestand downloadt, dat klaarstaat om zich via dit lek de toegang tot je computer te verschaffen", zegt Eddy Willems van het beveiligingsbedrijf G Data. "Vanaf dan kunnen ze er alles mee doen. Je kredietkaartgegevens ontfutselen, de computer bij een botnet voegen om grotere aanvallen op te zetten, andere pc's infecteren, de computer overnemen. En daar je dikwijls meerdere van die honderden mogelijk geïnfecteerde programma's gebruikt, hebben ze ook meer kans om op je pc te geraken. Dit is een van de ernstigste beveiligingsproblemen die we ooit zijn tegengekomen."

## Eerste aanvallen begonnen

Ondertussen zijn er al enkele hackeraanvallen via het pas ontdekte lek geseind. Enkele bedrijven kregen al een gerichte aanval op hun computernetwerk. Volgens Willems betekent dat ook dat hackers al methodes en software hebben ontwikkeld om een aanval uit te voeren. "We mogen er zeker van zijn dat cybercriminelen hier misbruik van zullen maken, zeker nu zowel het probleem als potentiële mogelijkheden om het te exploiteren publiek zijn gemaakt", zegt hij. "Maar wat me echt beangstigt, is: wat als het al eens gebeurd is? Er is geen manier om te weten hoe lang die informatie al voorhanden is. Misschien is het al eens gebruikt in een van de veertig miljoen virussen die we al achter de kiezen hebben, misschien is het informatie die tot nu toe veel geld waard was op de zwarte markt van cybercriminelen."

Als software volledig zonder programmeerfouten zou zijn, maakten cybercriminelen geen schijn van kans: ze zijn de achterpoortjes waarlangs ze hun aanval of virus op uw computer kunnen binnenleiden. Zogauw er een gat in de programmatuur van een softwareprogramma of besturingssysteem wordt ontdekt, kunnen booswichten daar even misbruik van maken. Tot de softwarefabrikant een update via het internet stuurt om het gat te dichten.

> **COMPUTEREXPERT EDDY WILLEMS (G DATA):**
> Dit is een van de grootste problemen die we ooit zijn tegengekomen

Het verschil tussen zo'n 'gewoon' beveiligingslek en hetgene waarover Microsoft nu alarm slaat, is echter erg groot: het pas ontdekte lek zit niet in de programmeercode van Windows zelf, maar in de manier waarop het besturingssysteem al meer dan twintig jaar werkt. Windows bevat honderden miniprogramma's die dll's heten (*'dynamically linked library'*), en die door verschillende programma's tegelijkertijd kunnen worden gebruikt. Daar zitten eigen programma's bij, maar ook software van derden of concurrenten, zoals Firefox en iTunes. Het probleem is dat hackers nep-dll's kunnen maken, ze op de computer van de gebruiker kunnen installeren, en er zo voor kunnen zorgen dat alle programma's die ze nodig hebben in één klap worden verziekt. "Een gewone programmeerfout geeft altijd een tijdelijk probleem", zegt Willems. "Wat we hier hebben is een designprobleem. Microsoft heeft Windows zo ontworpen dat verschillende programma's tegelijkertijd aan dezelfde Windows-componenten kunnen. Softwaremakers krijgen zelfs instructies om die samenwerking tussen hun programma's en Windows op de juiste manier te doen. Maar velen hebben die aan hun laars gelapt, en precies daar zitten nu alle programmeerfouten die kunnen worden misbruikt door hackers."

## Updates

Microsoft trok zelf aan de bel over het probleem, nadat een zogeheten 'ethische hacker' hen er vorige maand al op had gewezen. Het bedrijf legt nu de bal in het kamp van alle bedrijven die programma's voor Windows maken: "Dit probleem werd veroorzaakt door onveilige programmeerpraktijken", opperde een beveiligingsmelding van Microsoft. Het bedrijf stuurt geen algemene software-update voor zijn Windowsbesturingssystemen rond, omdat daardoor honderden programma's niet meer zouden werken. Alle fabrikanten moeten zelf een update uitsturen waarmee het gat in hun specifieke programma wordt gedicht. Maar dat is het net: omdat het over zoveel verschillende programma's gaat, wordt het versturen van updates om het gat te dichten geen sinecure. Willems: "De grote softwarefabrikanten zullen zich ongetwijfeld haasten. Apple, bijvoorbeeld, heeft ondertussen een update voor zijn programma's gedaan. Maar mijn vrees blijft voor de kleinere softwareprogramma's, die geen automatisch updatesysteem hebben. Daar zal de gebruiker zelf achter updates moeten gaan, en dat gebeurt in de praktijk erg zelden. Bovendien blijft er een probleem bij gebruikers met illegale software: die zijn niet geneigd updates te installeren, omdat de fabrikant hen zo kan ontmaskeren. Maar daardoor blijven ze kwetsbaar en leveren ze ook een groter risico om andere pc's te infecteren."

## Hoe beveiligt u uw computer het best tegen dit lek?

**De beste strategie om uw Windows-pc te beschermen tegen het nieuwe probleem, is zo snel mogelijk een degelijk beveiligingspakket te installeren. En vervolgens: afwachten. De beveiligingssoftware onderschept hackeraanvallen en virussen, terwijl de fabrikanten ondertussen koortsachtig werken aan een *patch* om het gat in hun product te dichten. Voor programma's van grotere fabrikanten gebeurt dat dus automatisch, andere software moet u zelf identificeren en ook zelf naar updates zoeken. U vindt een lijst van alle software die op uw computer staat geïnstalleerd door het 'Start'-menu open te gooien, daar 'Configuratiescherm' te kiezen, daaronder te klikken op 'Programma's' en tot slot op 'Programma's en onderdelen'. U krijgt een lijst te zien met alle software die op uw systeem staat. Nu begint het echte werk: voor al die programma's moet u op zoek gaan naar een update, op de website van de fabrikant.**

**"Beveiligingssoftware installeren neutraliseert aanvallen die werkelijk worden uitgevoerd, maar het lost het probleem niet op", zegt beveiligingsexpert Eddy Willems. "Het gat moet worden gedicht door, nadat de softwarefabrikanten zelf orde op zaken hebben gesteld, alle software op uw systeem up-to-date te houden."**

(RME)