Hackers plegen beursfraude met gekraakte Belgische rekeningen

Twintig Belgische beleggers die hun portefeuille online beheerden, hebben in 2007 zonder het zelf te weten beursfraude gepleegd op buitenlandse aandelenmarkten. De acties werden uitgevoerd door hackers die inbraken op hun account.

DOOR RONALD MEEUS

BRUSSEL ● 'Pump and dump'-fraude via hacking is de laatste drie jaar een internationale trend geworden op het vlak van computercriminaliteit. De aanvallen zijn kort, brengen tienduizenden tot honderdduizenden euro's op en worden pas erg laat ontdekt.

Het federaal parket onderzoekt al eventjes de hacking van de onlinebeleggingsportefeuille van twintig Belgische beleggers waarmee beleggingsfraude werd gepleegd. Het nieuws wordt bevestigd door de Commissie voor het Bank, Financie- en Assurantiewezen (CBFA), de Belgische financiële waakhond.

De hackings vonden plaats in juli 2007, in een periode waarin verschillende klanten van Belgische onlinebankingsystemen geteisterd werden door hackers van op een 'botnet', een netwerk van pc's dat eerder overgenomen werd door middel van een computervirus. Via dat netwerk werd malafide software geïnstalleerd op de pc's van de slachtoffers. Die ontfutselde hen hun gebruikersnaam en wachtwoord. Op die manier werd vervolgens 'pump and dump'-fraude gepleegd op buitenlandse aandelenmarkten. Via de gehackte accounts werden honderdduizenden kleine aandelen aangekocht, bij voorkeur op minder bekende en minder gecontroleerde internationale markten zoals de Amerikaanse 'over the counter'-beurs (OTC). Die plotse interesse stuwt de aandelenprijs dan omhoog, waarna de aangekochte aandelen weer even snel worden verkocht. Ondertussen maakt men tienduizenden euro's winst, die snel worden weggesluisd.

'Pump and dump'-fraude via computerinbraak is de afgelopen drie jaar een trend geworden in de computercriminaliteit. Dat komt omdat de aanvallen in korte tijd relatief veel geld opbrengen: in één uur tijd kan de koers van een aandeel danig worden opgepompt dat de criminelen er 20.000 tot 100.000 euro mee verdienen. Bovendien duurt het ook wel eventjes vooraleer de fraude opvalt. Meestal gaat het immers om de door de grote beleggersgemeenschap genegeerde pennystocks, aandelen van enkele dollarcenten, van bedrijven die weinig aandacht krijgen van beleggers of op de rand van de afgrond staan. Tegen de tijd dat er een onderzoek wordt ingesteld, is de slag al lang binnen.

> EDDY WILLEMS (COMPUTERBEVEILIGING EICAR):
> 'Pump and dump'-fraude is een methode die momenteel erg populair is

"Het gebeurt allemaal onder de radar en de daders zorgen er ook voor dat dit zo blijft", zegt Eddy Willems, vicedirecteur van de Europese computerbeveiligingsorganisatie Eicar. "Zo staken ze hun aanvallen tijdelijk als de koers van een bepaald aandeel te snel is gegroeid. Liever spreiden ze enkele kleinere aanvallen over een paar weken of een maand. Dat maakt hen moeilijker detecteerbaar."

FOTO CORBIS

■ 'Pump and dump'-fraude lijkt een trend bij hackers. In één uur tijd kan de koers van een aandeel zo worden opgepompt dat men er tot 100.000 euro mee verdient.

De acties worden ondernomen door wijdvertakte internationale bendes die opereren vanuit India, China, Rusland of voormalige Oostbloklanden. In 2008 werden al drie Indiase mannen gearresteerd die via een soortgelijke hackingfraude zestig Amerikaanse onlinebeleggers hadden gedupeerd. Enkele maanden geleden stelde de Securities and Exchange Commission (SEC), de Amerikaanse tegenhanger van de CBFA, een onderzoek in naar een Russische belegger die via deze methode honderdduizenden dollars aan illegale beurswinsten bij elkaar had gesprokkeld op kleinere Amerikaanse aandelenbeurzen. Op een bepaald moment, zo stelt het onderzoek, had hij meer dan 140.000 dollar (115.000 euro) verdiend in minder dan een kwartier.

Volgens de CBFA werden ook de Belgische aanvallen door zo'n internationale bende gepleegd en waren de aandelen in kwestie eveneens buitenlands. "Er zijn altijd een paar internationale bendes tegelijkertijd bezig", zegt Willems. "Het is een methode die momenteel erg populair is."

Slachtoffers vergoed

De twintig Belgische slachtoffers verloren door de hacking ook de fondsen die al in hun portefeuille zaten. Het zou gaan om een totaal van ongeveer 100.000 euro. Ze kregen de fondsen inmiddels terugbetaald door hun bank, aldus de CBFA. Alle computerinbraken gebeurden via het webbankingsysteem van de slachtoffers, maar die werden op zich niet gekraakt. De inloggegevens werden buitgemaakt via een rechtstreekse inbraak op de pc van de slachtoffers zelf.

Toch heeft de CBFA al een initiatief genomen om webbankingsystemen veiliger te make<y. "Een gebruikersnaam en een wachtwoord alleen volstaan niet meer. Ze moeten een technologie hanteren die de systemen per inlogsessie beveiligt, zoals een Digipasstoestelletje."