Mysterieus Confickervirus kan vandaag volgens sommige experts het volledige internet platleggen

D-day voor 10 miljoen computers

Het bijzonder hardnekkige Confickervirus, dat wereldwijd meer dan tien miljoen computers heeft besmet, komt vanaf vandaag opnieuw onder de controle van zijn makers. Hoewel het evengoed om een aprilgrap kan gaan, is het virus volgens computerexperten tot alles in staat, tot zelfs de complete vernietiging van het internet.

DOOR RONALD MEEUS

BRUSSEL • Het Confickervirus, dat in november 2008 opdook, is ook het hardnekkigste virus ooit, omdat het zichzelf kan updaten via het internet: het weet zichzelf bijzonder snel te beschermen tegen alle nieuwe beveiligingssoftware die het van de computer probeert te wissen.

Voor een computervirus van zijn aard en omvang is het Confickervirus tot nu toe opvallend ongevaarlijk gebleven. Het doet voorlopig niets met de pc's die het heeft besmet, behalve hardnekkig standhouden tegen de beveiligingssoftware die op die computers wordt geïnstalleerd door middel van constante updates, en zichzelf zo ruim mogelijk verspreiden.

Maar dat verandert vanaf vandaag. Beveiligingsexperten die de programmatuur van het virus onderzoeken, ontdekten dat het vandaag stopt met zich te vermenigvuldigen en wacht op instructies vanaf een vreemde computer. Wanneer die doorgave van instructies precies gebeurt, is onbekend: het virus kan vandaag al worden geactiveerd, maar dat kan voor hetzelfde geld pas binnen een week zijn. Ook wat die instructies precies kunnen zijn weet niemand, want de architecten van het virus zijn tot nu toe onbekend.

"We hebben eigenlijk niet het minste idee wat er kan gebeuren", zegt analist Eddy Willems van het computerbeveiligingsbedrijf Kaspersky. "Het is eigenlijk de eerste keer dat we zo in het ongewisse blijven: meestal geven de programmatuur en het gedrag van een virus wel een idee van wat het van plan is. Conficker niet: het is een van de grootste computervirussen die we tot nu toe hebben gezien, en er zit duidelijk een meesterplan achter, maar het blijft gissen wat het doet tot er effectief iets gebeurt."

Armageddon

De hardnekkigheid van het virus leidde al tot de wildste speculaties. Dat het bijvoorbeeld door een overheid in het leven is geroepen, en binnenkort zal worden gebruikt voor een cyberoorlog: een massieve internetaanval die de volledige infrastructuur van een land kan platleggen. Er wordt zelfs hier en daar gevreesd voor een totaal armageddon van het internet. In 2002 wist een veel minder krachtig netwerk van geïnfecteerde computers twee van de dertien 'rootservers' lam te leggen, supercomputers die de pijlers vormen onder het volledige internet. Als het merendeel daarvan wordt uitgeschakeld, is de kans erg groot dat de overblijvende rootservers de wereldwijde internettrafiek niet meer aankunnen, met als gevolg niks minder dan een totale crash van het internet.

"Als de mensen achter het Confickervirus erin slagen om de controle over al die miljoenen geïnfecteerde computers over te nemen en een aanval zouden inzetten op die rootservers, zou het theoretisch mogelijk zijn om er een aantal van plat te leggen", zegt Willems. "Maar onze schatting is dat ze slechts één procent van alle besmette computers zullen kunnen activeren: ondertussen hebben ook gebruikers met een besmette pc de nodige beveiligingssoftware geïnstalleerd, die wellicht de activering van het Confickervirus kan tegenhouden."

> Analisten laten alle mogelijkheden open: cybercrime, fataal virus of aprilgrap

Zonder internet geen fraude

Bovendien is het, zelfs wanneer dat theoretisch mogelijk is, onwaarschijnlijk dat de makers de volledige infastructuur van het internet proberen plat te leggen. "De meeste virussen worden tegenwoordig door de georganiseerde misdaad verspreid, met het doel om er geld mee te verdienen", zegt Willems. "Als ze de infrastructuur aanvallen, gaat dat niet meer: zonder internet is er ook geen internetfraude."

Voor computercriminelen zijn er verschillende manieren om geld te verdienen aan zo'n massief netwerk van geïnfecteerde computers. Ze kunnen worden gebruikt om een massale campagne van ongewenste reclamemails (spam) te lanceren, de kredietkaartgegevens van hun gebruikers te ontfutselen, of een gerichte internetaanval uit te voeren op verscheidene kleinere doelwitten. Wat ook dikwijls gebeurt, zo menen computerbeveiligers, is dat de maker van het virus het netwerk van geïnfecteerde computers (het zogeheten 'botnet'), of stukken ervan, verkoopt aan computercriminelen, die er vervolgens de echte slag mee slaan.

"We denken allemaal eerder aan computercriminaliteit, en daarin zijn er verscheidene scenario's mogelijk", zegt Willems. "De wereldwijde paniek rond Conficker wordt bijvoorbeeld zelf al geëxploiteerd. Er duiken de laatste weken 'Conficker removal tools' op het internet op, programma's die zogenaamd het virus van je computer verwijderen, maar in plaats daarvan een echte hacking op je computer uitvoeren. Oppassen daarmee."