



'Virusschrijvers zijn professionals'

Het is slechts een kwestie van tijd voordat virussen op mobiele telefoons echt gaan toeslaan. Dit zal gebeuren als virusschrijvers hebben ontdekt hoe ze er geld mee kunnen verdienen.

Door Webwereld redactie | Webwereld | 10 nov 2005

mikkohypponeninline

"Virusschrijvers zijn nu op zoek naar virussen die zich zonder medeweten van de gebruiker installeren en doorsturen. Ook wordt er gezocht naar een manier om direct geld aan iemand te verdienen waarbij het virus ongemerkt een grote hoeveelheid mms-berichten verstuurt, een ringtone bestelt of een duur telefoonnummer belt", zegt Mikko Hyppönen, *chief research officer* bij virusbestrijder F-Secure, in een interview met Webwereld.

Mobiele virussen hebben tot nu toe maar relatief weinig apparaten besmet. Dat komt omdat de gebruiker vaak nog een handeling moet verrichten voordat een virus wordt geïnstalleerd en omdat er diverse mobiele besturingssystemen in gebruik zijn.

"Pas als virusschrijvers een manier hebben ontdekt om geld te verdienen met het maken van *malware* voor mobiele telefoons, zullen de mobiele virussen echt gevaarlijk worden. Het is nog niet zo ver, maar dat gaat zeker gebeuren", stelt Hyppönen.

Vijanden

Hyppönen werkt nu bijna vijftien jaar voor F-Secure. "Toen ik begon in 1991 waren er nog maar 300 virussen. Nu zijn dat er 140.000. En dagelijks komen er nog veertig bij."

De grootste verandering tussen toen en nu zit 'm in de 'vijanden', de virusschrijvers. "Die zijn veranderd en hun motief is ook veranderd", aldus de Finse beveiligingsexpert. "De macrovirussen en e-mailwormen werden vooral gemaakt door tieners en scriptkiddies. De netwerkwormen van tegenwoordig worden gemaakt door professionals."

Het interessantste voorbeeld hiervan is de Bagle-worm die in 2004 voor het eerst de kop op stak en waarvan nu 27 varianten bekend zijn. "De Bagle-worm zit zo complex in elkaar. Dat is een virus waarin een client server architectuur is ingebouwd. Dat kan niet door hobbyisten zijn gemaakt. Dat is een groep professionals geweest die daar enorm veel geld mee verdient."

Virusschrijvers proberen met de virussen zoveel mogelijk pc's te veranderen in zombie-pc's of botnets. Hierbij wordt een achterdeur in de pc ingebouwd die op elk moment gebruikt kan worden om spam en phishing-mailtjes te versturen. Die botnets worden te koop aangeboden aan spammers en oplichters, aldus Hyppönen.

Skype-virus

Door het gebruik van botnets worden virusschrijvers ook steeds moeilijker om te achterhalen. Bovendien maken spammers en oplichters veel gebruik van hostingproviders in China of in andere landen waar nog geen wetten tegen internetcriminaliteit zijn. De huidige wet- en regelgeving vormt een probleem bij de vervolging van deze criminelen, vindt Hyppönen. "We hebben een wereldwijd netwerk, maar geen wereldwijd geldende wetten."

Volgens Hyppönen bestaat de nieuwe generatie virussen uit mobiele virussen waarmee geld te verdienen valt en virussen die binnenkomen via programma's die niet door firewalls geblokkeerd worden. "Te denken valt daarbij aan de browser, mail, instant messaging en bijvoorbeeld Skype. Ik kan me voorstellen dat er een virus komt dat pc's infecteert via Skype en zich verspreidt via de contacten van dat programma. Het is er nog niet, maar het zou wel kunnen."