

Keylogging steeds populairder

November 2005

Henk Jongedijk, maandag 23 oktober 2006 - 07:38:16

Het verschijnsel keylogging is niet echt nieuw, want in 2000 werden al keyloggers gesignaleerd. In maart 2005 werd in onderzoeken aangetoond dat keylogging 'echt' in opmars is.

Wat is keylogging nu precies? Het betreft software die wordt gebruikt om toetsaanslagen van computergebruikers te registreren. De software wordt niet vrijwillig geïnstalleerd, maar wordt stiekem meegestuurd met computer virussen en -wormen. Het keylog programma registreert zonder dat de gebruiker het merkt iedere toetsaanslag op de computer. Deze informatie wordt doorgeseind aan de cracker, die hier op zijn beurt gevoelige informatie uit kan filteren.

Keylogging-software wordt in de meeste gevallen verstuurd via zogenoemde phishing-mails, die internetters naar gekopieerde sites van bekende ondernemingen of instanties lokken (bijvoorbeeld Postbank, eBay, Paypal, Microsoft). De internetters worden vervolgens verzocht gegevens als creditcardnummers of pincodes op te geven. Criminele organisaties worden zo in staat gesteld op grote schaal te frauderen.

Het aantal varianten van keyloggers is volgens onderzoekers de afgelopen jaren explosief gestegen. In 2000 werden 'slechts' 300 keyloggers ontdekt. Dit aantal daalde het jaar daarop zelfs tot 275.

De echte stijging in het gebruik van keyloggers vond plaats in 2002 en 2003. Het aantal steeg toen van 444 naar 1230. Ook in 2004 groeide het gebruik nog flink, met in totaal 3753 keyloggers. De teller blijft in 2005 naar verwachting net onder 6200 steken. Volgens beveiligingsonderzoekers van iDefense zijn er dit jaar zo'n 6000 keyloggers in omloop gebracht. Dat is een stijging van 65 procent vergeleken met vorig jaar.

De stijging van het gebruik van deze zogeheten keylogging-software wordt waarschijnlijk veroorzaakt doordat computergebruikers steeds onvoorzichtiger worden. Een andere oorzaak is dat online bankieren tegenwoordig gemeengoed wordt, proberen crackers steeds vaker gevoelige gegevens te achterhalen met behulp van de zogenaamde keyloggers. Een derde verklaring is de groeiende internationale handel in gestolen creditcardgegevens.

Wat kan ik als gebruiker tegen phishing en keylogging doen? Installeer recente anti-virus software en voer regelmatig een scan uit. Tevens kan goede anti-virus software verdacht gebruik van de communicatie-poorten van uw computer in de gaten houden en signaleren. Een andere goede tip is om altijd op letten of u echt met degene zaken doet waarmee u denkt zaken te doen. Vooral bij Internet bankieren dient er in uw browser het volgende Internet adres te staan: <https://uwbank.nl> waarbij https betekent dat uw gegevens over een beveiligde verbinding worden verzonden. Dubbelklik vervolgens op het slotje onderin uw browser. Het certificaat dient verleend te zijn aan de bank waarmee u zaken doet. Wordt niet aan deze voorwaarden voldaan of twijfelt u, neem dan contact op met uw bank.

Bronnen:

<http://www.webwereld.nl/articles/38393>http://www.idefense.com/about/newscenter/recentreleases/2005_11_15.jsp<http://www.edusite.nl/edusite/nieuws/14466><http://www.websensesecuritylabs.com/resource/PDF/APWGPhishingActivityReportMarch2005.pdf><http://www.breekpunt.nl/nieuwsbericht.asp?id=10388><http://www.websense.com/><http://www.webuser.co.uk/specials/63198.html>