Worm Swen@mm vermomt zich als Microsoft update mail
Oktober 2003
Henk Jongedijk, maandag 23 oktober 2006 - 00:00:00

De e-mail berichten die de W32.Swen@mm Internetworm verspreidt lijken rechtstreeks afkomstig van Microsoft. Het bericht is in html opgemaakt en doet zich voor als een patch-informatie bericht van Microsoft.
In werkelijkheid is het een geniepig gevaarlijke worm, die zelf via een vernuftige weg emailtjes verstuurt naar alle email adressen die het op uw computer aantreft zodra u besmet bent. Met uiteraard dezelfde misleidende boodschap, zodat uw vrienden en bekenden binnen de kortste keren ook besmet kunnen raken.

Zelf kreeg ik de afgelopen week (op 28 en 29 september 2003) in totaal drie mailtjes binnen, terwijl mijn provider bekend staat om de goede spam filters en uitstekende virus detectie. Dit geeft tegelijkertijd ook aan hoe ernstig dit wormvirus is.

Verspreiding via e-mail geschiedt via zowel Outlook (standaard SMTP) als via een eigen SMTP-engine. Indien het virusbericht wordt verzonden via de eigen SMTP bevat de virusbijlage een codering die ervoor zorgt dat het e-mailbericht bij binnenkomst in het mailprogramma van de ontvanger automatisch wordt geopend in de zogenoemde voorbeeldweergave.

Het is aan te raden om sowieso hiervoor patches te installeren. Dit kan eenvoudig via de Windows-update functie of op
http://windowsupdate.microsoft.com/

In andere gevallen wordt het virus geactiveerd door het (bijlage) bestand handmatig te openen.

De belangrijkste schade-componenten zijn:
- De-activeren van geinstalleerde security-software.
- Weergeven van tal van Windows-vensters.
- Installatie van een aantal bestanden.
- Toevoeging van een aantal registry-regels.

Eigenschappen van het e-mailtje
Onderwerpen: (wisselend, mogelijk Ã © Ã ©n van onderstaande:)
OF/OF:
- New Microsoft Patch
- Current Microsoft Critical Patch
- Network Security Patch
- Last Microsoft Security Pack
- Last Critical Pack
- New Security Upgrade

- Bijlagebestand 104 KB groot: (wisselend van naam, mogelijk Ã © Ã ©n van onderstaande:)
(altijd met extensie .exe)
- Install897.exe
- installation???.exe (??? = 3 willekeurige karakters)
- Patch???.exe (??? = 3 willekeurige karakters)

- Upgrade.exe
- Q??????.exe (?????? = 6 willekeurige karakters) 104 Kb

Teksten van het bericht (wisselend): engelstalig met het verzoek de bijlage te installeren in verband met de "October 2003, Cumulative Patch". (In september was het "September 2003, Cumulative Patch" ...)

Brengt mij tot de trieste conclusie dat makers van virussen, trojaanse paarden en wormen helaas altijd geprikkeld blijven om dit soort programma's te bedenken, zolang er mensen blijven bestaan die niet geheel up-to-date zijn en daarom een mogelijke prooi vormen.

Ook de (fictieve) afzenders van het email bericht verraden dat het mailtje niet werkelijk van Microsoft afkomstig is.
In mijn geval waren de afzenders respectievelijk:

» MS Internet Security Department [gfmxgwkr@confidence.microsoft.net]

» Microsoft Corporation Network Security Department [dpqohx_ewuzfdg@advisor.msn.net]

» Microsoft Corporation Internet Security Division [sicdjmhzdb@technet.msn.net]

Opvallend is dat de gefingeerde Microsoft adressen op .net eindigen, terwijl iedereen weet dat Microsoft alom vertegenwoordigd is op .com websites.

Besteed daarom genoeg tijd aan het bestuderen van uw binnenkomende mail. Installeer nooit zomaar een aan u gestuurd programma, zonder dat u de bron kent.

Hoe verwijdert u het virus?
Bezoek Ã © Ã ©n van de onderstaande sites om uw pc te scannen en/of virus vrij te maken.

http://securityresponse.symantec.com/avcenter/venc/data/w32.swen.a@mm.html

http://www.bitdefender.com/bd/site/virusinfo.php?menu_id=1&v_id=158

Aanvullende informatie / links
perbericht Microsoft 18 september 2003
column januari 2003: 2002 Jaar van virus Yaha
column december 2002: Heb ik een virus, worm, hoax of Trojaans paard?
column december 2001: Worstelen met wormen
column oktober 2002: Hoax: moderne kettingbrief

Voorbeelden van binnenkomende SWENN@MM berichten

-