Angriffswelle auf private Homepages

Mehrere zehntausend deutsche Webauftritte wurden mit Trojanern infiziert. Links in Spam-Mails führen zu dem als Flash-Player-Update getarnten Schädling. Viele Webmaster dürften den Einbruch noch nicht bemerkt haben.

Meldung vom 31.07.2008

Seit einer Woche tauchen vermehrt Spam-Mails auf, die aufgrund einer knapp gehaltenen Schlagzeile und einem Link zu einer unverdächtigen Homepage durch die Maschen der Spam-Filter von Thunderbird und Spam-Assassin schlüpfen.

Die Links führen auf die Homepages von ahnungslosen Inhabern, auf denen die Spammer offenbar unbemerkt eine HTML-Datei mit vermeintlich kostenlosen Videos und eine Windows-.exe-Datei hinterlegt haben. Besucher erhalten die Meldung, dass zur Darstellung der Videos ein Update des Flash-Player erforderlich sei. Anschließend bekommen sie die Datei get_flash_update.exe zum Download angeboten, in der ein Trojaner steckt. Bei dem Trojaner handelt es sich um eine neue Variante des Trojan-Downloader.Win32.Agent.yhp, die derzeit von einigen verbreiteten Virenscannern noch nicht erkannt wird.

Von dem Angriff sind Homepages bei verschiedenen Webspace-Anbietern betroffen. Allein beim Hoster 1&1 ist in den vergangenen vier Tagen eine starke Zunahme der Angriffe beobachtet worden, bis zu 20.000 Kunden hätten den Schädling in ihrem Webspace. Der Angriffsweg sei jedoch noch nicht lückenlos aufgeklärt: "Schuld könnten Keylogger auf den PCs der Kunden oder unsichere FTP-Passwörter sein", sagte Andreas Maurer, Pressesprecher von 1&1, gegenüber heise Security. Bei einzelnen Accounts seien sehr leicht erratbare FTP-Passwörter festgestellt worden. Bei betroffenen Internetauftritten wurden bereits die FTP-Passwörter geändert und die Kunden informiert.

Ob eine Website betroffen ist, können Webmaster unter anderem an der Existenz der Datei get_flash_update.exe im Document-Root-Verzeichnis erkennen. Darüber hinaus liegt dort eine HTML-Datei, die das vermeintliche Update per Javascript auf den Benutzerrechner downzuloaden versucht. Sie trug in einer ersten Spamwelle den Namen default.html, seit gestern vermehrt showvideo.html. Die Funktion der Website wird in der Regel nicht beeinträchtigt, sodass der Schädling normalen Besuchern – die die Seite nicht über den Link aufrufen – oder dem Inhaber in der Regel nichts auffällt. Betroffene Webmaster bei anderen Hostern sollten zumindest das FTP-Passwort ändern und diese Dateien löschen.

(Johannes Kiehl) / (dab/c't)