Conficker-Wurm stört legitime Domains im März

Eigentlich produziert der Domain-Algorithmus des millionfach verbreiteten Wurms nur zufällige Buchstabenfolgen, doch einige davon sind legitime und hochfrequentierte Domains und nun vom Ausfall bedroht.

die News-Meldung vom 01.03.2009

Der Conficker-Wurm wird im März mindestens vier legitime Domains stören, heißt es in einem Bericht des Antivirus-Herstellers Sophos. Zwar bestehen die Domain-Namen, die der Schädling nutzt, um für neue Befehle nach Hause zu telefonieren, gewissermaßen aus einer zufälligen Buchstabenkombination und sind daher größtenteils ungenutzt. Doch am 8. März lautet die Zeichenkombination zufällig jogli.com – die Domain einer Musiksuchmaschine.

Am 13. März werden die Conficker-Drohnen die Southwest-Airlines-Website wnsux.com mit Anfragen überhäufen. qhflh.com, die Domain eines Frauennetzwerkes der chinesischen Provinz Qinghai, ist am 18. März an der Reihe und die praat.org, deren Inhalt sich mit algorithmischer Audio-Analyse beschäftigt, wird am 31. März zur Wurmhochburg. Den Domains droht durch die unnützen Netzwerkverbindungen der Millionen infizierten Systeme für rund einen Tag der Totalausfall. Laut Sophos sollen auch andere weniger frequentierte legitime Domains auf dem Weg des Wurms liegen.

Der AV-Hersteller schlägt vor, dass die betroffenen Sites ihre Domain für den Tag im DNS-System stilllegen oder die HTTP-Anfrage

http://<domainname>/search?q=<N>

herausfiltern sollen.

Die erste Option erfordert, dass der Betreiber eine Ausweich-Domain parat hat. Southwest-Airlines-Besucher können beispielsweise vorübergehend den alternativen Domain-Namen southwest.com verwenden. Die zweite Option dürfte nur in Frage kommen, wenn die angefragte Such-URL nicht verwendet wird.

Microsoft, ICANN und andere an der Conficker-Blockierung beteiligten Firmen – auch bekannt als das Conficker-Kabal – registrieren vorab die Domains, die der Schädling künftig sein Zuhause nennen wird. Der Algorithmus, nach dem der Wurm die Zeichenfolgen generiert, ist inzwischen bekannt. In diesem Zusammenhang weist Sophos darauf hin, dass einige der Domains bereits registriert seien und zum Verkauf stünden. Die Liste der zu blockenden Domains ist daher unvollständig, da sie vergebene Domains aus rechtlichen Gründen nicht enthalten darf.

(c't)

die heise Security News der Zeitschrift c’t

www.heise.de/security