Studie: 2,5 Millionen PCs mit Conficker-Wurm infiziert

Da der Wurm die Fähigkeit zum Nachladen von Code habe, sei demnächst wahrscheinlich mit einem größeren Botnetz zu rechnen. Viele der infizierten PCs sollen in Unternehmensnetzwerken stehen.

die Meldung vom 14.01.2009

Nach Schätzungen des Antivirenherstellers F-Secure hat der Windows-Wurm Conficker alias Downadup bereits rund 2,5 Millionen PCs infiziert. Da der Wurm die Fähigkeit zum Nachladen von Code habe, sei demnächst wahrscheinlich mit einem größeren Botnetz zu rechnen. Von welchen Domains der Wurm den Code nachlädt, bestimmt er laut F-Secure über einen komplizierten Algorithmus. Dabei generiere er viele verschiedene mögliche Domainnamen, sodass ein Sperren aller kaum möglich sei.

F-Secure hat nach eigenen Angaben aber einige Domains vorab selbst registriert und beobachtet, wieviel infizierte Maschinen die Domains aufrufen. Damit sei zwar auch die Kontrolle über die Maschinen möglich, bis hin zum Desinfizieren, aus rechtlichen Gründen greife man aber nicht auf die PCs zu.

Viele der Domain-Aufrufe kämen aus Unternehmensnetzwerken, bei denen man aufgrund der Adressumsetzung mit NAT nur eine einzige IP-Adresse sehe. Dahinter könnten aber in Wirklichkeit mehrere tausend infizierte PCs stehen. F-Secure hat in einem Blog-Eintrag die Aufrufe der Domains nach Ländern aufgeschlüsselt.

Aktuell sind drei Varianten des Conficker-Wurms unterwegs. Die B- und C-Varianten sollen nicht nur die RPC-Sicherheitslücke in Windows ausnutzen, sondern zudem versuchen, in Systeme mit einem schwachen Administrator-Passwort einzudringen. Dazu probieren sie eine Liste bestimmter Passwörter durch. Darüber hinaus verbreitet sich der Wurm auch über USB-Sticks. Schutz vor dem Wurm bietet also nicht nur die Installation des Sicherheits-Updates von Microsoft, zusätzlich sollten Administratoren auch schwache gegen starke Passwörter auswechseln.

Zuletzt wurde bekannt, dass der Wurm Computer der Kärntner Landesregierung und die PCs der Kärntner Krankenanstaltengesellschaft KABEG in mindestens drei Krankenhäusern befallen hatte.

[Update] Zusammen mit den gestern veröffentlichten Sicherheits-Updates für eine neue Lücke in Windows verteilt Microsoft eine aktuelle Version des Malicious Software Removal Tool, das den Wurm erkennen und eliminieren soll. **[Update]**

(c't)

die heise Security News der Zeitschrift c’t

www.heise.de/security