Keylogger unter die Lupe genommen

Forscher haben eine Fallstudie zu Bank-Trojanern, Keyloggern, den dabei gestohlenen Daten und den dazugehörigen Datensammelstellen (Dropzones) veröffentlicht.

die Meldung vom 18.12.2008

Ein Team um den Honeynet-Spezialisten Thorsten Holz von der Universität Mannheim hat eine Fallstudie zu Bank-Trojanern, Keyloggern und deren Datensammelstellen (Dropzones) veröffentlicht. Die Forscher haben mehrere der Schädlinge und deren Aktivitäten über einen längeren Zeitraum beobachtet und dabei mehr als 33 GByte an Logdaten von mehr als 70 unterschiedlichen datenstehlenden Schädlingen in den Dropzones gefunden.

Die Logdaten enthielten persönliche Informationen von mehr als 170.000 Opfern wie Passwörter, PINs, Benutzernamen und ähnliche Daten. Darunter fanden sich auch mehr als 10.000 Bankkontodaten inklusive PINs, mehr als 140.000 E-Mail-Passwörter und fast 80.000 Zugangsdaten zu Social-Networking-Seiten wie Facebook und Hi5.

Den Keylogger Limbo hat das Team einer näheren Analyse unterzogen. Insgesamt beobachteten sie rund 164.000 Infektionen mit dem Schädling, wobei der Keylogger den größten Teil der gesammelten Daten in zwei chinesischen Dropzones hinterlegte. 16 Prozent der Infektionen waren Russland zuzuordnen, 14 Prozent den USA, 13 Prozent Spanien, 12 Prozent Großbritannien und immerhin rund 7 Prozent Deutschland.

In seiner 22-seitigen Studie gehen die Forscher auch auf die Werte der gestohlenen Daten ein. Je nach Liquidität ist ein Bankkonto für 10 bis 1000 US-Dollar zu haben. Kreditkarten scheinen langsam zu Ramschware zu verkommen: Bereits für 40 US-Cent kann man die Daten einer Karte kaufen. E-Mail-Passwörter nehmen an Wert zu und kosten zwischen 4 und 30 US-Dollar. Der komplette Bericht "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones" steht zum Download bereit.

Im Anschluss an die Studie hat das Team alle Logdaten an das australische CERT (AusCert) übergeben, die über ein System verfügen, die Informationen an Banken und andere Institutionen weiterzuleiten. Diese können dann die Opfer informieren und weitere Maßnahmen einleiten.

(dab/c't).