

Freitag, 25.07.2008, Handelsblatt.de

Gefälschte Zoll-E-Mail öffnet Trojaner

Internet-Käufer aufgepasst: Eine gefälschte E-Mail vom Zoll, nach der angeblich ein Paket zur Abholung wartet, verbirgt einen geschickt getarnten Trojaner. Davor warnt der Sicherheitsdienstleister Avira.

Laut Avira sieht das Ganze derzeit so aus:

Die Spam-Mails tragen als Betreff die Zeile "Parcel requires declaration". Es sei angeblich ein Formular auszufüllen.

Text:

"Good day, We have received a parcel for you, sent from France on July 9. Please fill out the customs declaration attached to this message and send it to us by mail or fax. The address and the fax number are at the bottom of the declaration form.

Kind regards,
Lucinda Addison
Your Customs Service"

Der Dateianhang der E-Mail trägt den Namen Bill-Tax.zip. Das Archiv enthält die Datei "Bill_Tax_____N89798742344.exe". ...

Windows zeigt bei der Datei das Symbol eines Word-Dokuments an, selbst für die Spam-gewohnten Avira-Leute eine pfiffige und perfektionierte Tarnung.

Der als Tr/Spy.ZBot.dkx erkannte Schädling legt bei der Ausführung eine Kopie von sich selbst im Windows-Verzeichnis unter dem Namen ntos.exe ab. Er versteckt sich nach dem Systemstart mit Rootkitfunktionen, indem er Code in die Windows-Systemdatei winlogon.exe injiziert.

Zudem verbindet er sich mit einem Server im Internet und lauscht auf eingehende Pakete. Weiterhin spioniert der Trojaner den Anwender aus. Außerdem lädt der Schädling aus der ZBot-Familie weitere Komponenten nach. Den heruntergeladenen Schädling erkennt Avira als TR/Dldr.Agent.xft.

10:49