# Millionenfacher Passwortklau durch Würmer

**Die letzte Version des Malicious Software Removal Tools entdeckt neuerdings spezielle Schädlinge, die es auf Zugangsdaten zu Online-Spielen abgesehen haben. Sie wurde auf Anhieb auf über einer Million Rechnern fündig.**

News die Meldung vom 23.06.2008

Nicht immer haben es Computerschädlinge auf Zugangsdaten zu eBay, PayPal oder Online-Banking abgesehen. Eine spezielle Gattung klaut gezielt Passwörter zu Online-Spielen – und das offenbar mit großem Erfolg. Zum vergangenen Patchday hat Microsoft in das Malicious Software Removal Tool (MSRT) spezielle Erkennungsfunktionen für die Schädlinge Taterf, Frethog und Co eingebaut. Die zurückgemeldeten Scanergebnisse verblüfften selbst die einiges gewöhnten Malware-Spezialisten in Redmond.

Allein am ersten Tag entfernte das MSRT Taterf von 700.000 Systemen. Zum Vergleich: Den Bot-Netz-Client des berüchtigten Sturmwurms fand das Tool im ganzen ersten Monat nach Einbau der Signaturen nur halb so oft. Viele Online-Spiele wie Lineage Online und Legend Of Mir sind vor allem im Fernen Osten populär. Das spiegeln auch die MSRT-Statistiken wieder, die allein eine halbe Million infizierter Systeme in China ausmachen. Doch World of Warcraft und Valves Steam Client haben es auch in der westlichen Hemispäre zu einiger Verbreitung gebracht, sodass die 230.000 spanischen Systeme auf Platz drei nicht verwundern; Deutschland taucht in der Top-Ten-Liste allerdings nicht auf.

Dabei verbreiten sich Taterf und Konsorten laut Microsoft eher gemächlich, indem sie sich auf alle erkannten Laufwerke kopieren und dort eine passende Autorun-Datei autorun.inf anlegen. Entgegen der Darstellung in Microsofts Threat Research & Response Blog genügt es allerdings nicht, einen infizierten USB-Stick an ein Windows-System anzustecken, um es zu infizieren. Denn USB-Sticks und MP3-Player melden sich üblicherweise als DRIVE_REMOVABLE, und für diesen Laufwerkstyp ist Autorun unter XP standardmäßig abgeschaltet. autorun.inf kann lediglich dafür sorgen, dass im automatisch angezeigten Autoplay-Dialog eine Option wie "Zeig mir die fetten Bilder" als Default-Eintrag erscheint. Der Anwender muss diese Aktion jedoch manuell bestätigen, was aber offenbar keine ausreichende Hürde ist, um eine Infektion zu verhindern.

Um Autoplay zu deaktivieren, ist unter XP ein Eingriff in die Registry erforderlich, den Microsoft auf seinen Supportseiten beschreibt. Vista bietet Einstellmöglichkeiten für "Automatische Wiedergabe" in der Systemsteuerung.