Säuberung eines infizierten Windows-Betriebssystems auf Basis von Malware-Analyse-Berichten

Alexander Knaus Johannes Stüttgen Jan Göbel
Markus Engelberth Felix C. Freiling

{alex.knaus|johannes.stuettgen}@googlemail.com
{goebel|engelberth}@uni-mannheim.de

Abstract: Wir stellen einen Ansatz vor, wie man Systeme, die durch Schadsoftware infiziert sind, automatisiert säubern kann. Grundlage für die Säuberung ist ein Malware-Analyse-Bericht, der durch eine dynamischen Analyse des Schadprogramms mit Hilfe eines Sandbox-Systems erstellt werden kann. Aus diesem Bericht werden die Informationen über die durch das Schadprogramm vorgenommenen Systemveränderungen gewonnen. Wir präsentieren die Ergebnisse einer prototypischen Umsetzung des Ansatzes, der für einen Großteil heute existierender Schadprogramme gut funktioniert.