# 通用、有效且轻量的PowerShell解混淆和语义敏感的攻击检测方法

熊春霖[1]，李振源[1]，陈焰[2]，朱添田[3]，王箭[1]，杨海[4]，阮伟[5]
[1]浙江大学计算机科学与技术学院，中国杭州市，310027
[2]西北大学电气工程与计算机科学系，美国伊利诺伊州埃文斯顿市，60208
[3]浙江工业大学计算机科学与技术学院，中国杭州市，310023
[4]杭州奇盾信息技术有限公司，中国杭州市，310027
[5]浙江大学控制科学与工程学院，中国杭州市，310027

**摘要：**近年来，PowerShell攻击越来越多见诸报道。然而，由于PowerShell语言的动态特性，且可在不同级别构造脚本片段，即使基于最先进的静态脚本分析的PowerShell攻击检测方法，其本质上也容易受到混淆的影响。本文为PowerShell脚本设计了一种通用、有效且轻量的去混淆方法。首先，为精准识别模糊脚本片段，根据混淆方法对PowerShell抽象语法树的影响，提出一种全新混淆片段检测方法，在此基础上提出一种基于仿真的恢复技术。此外，设计了一个语义敏感的PowerShell攻击检测系统，该系统利用经典的面向目标的关联挖掘算法，新识别31个用于恶意脚本检测的语义特征。在2342个良性样本和4141个恶意样本上的实验结果表明，所提去混淆方法平均耗时不到0.5秒，且将模糊脚本和原始脚本的相似度从0.5%提至93.2%。采用该去混淆方法，Windows Defender和VirusTotal的攻击检测率分别从0.33%和2.65%提至78.9%和94.0%。实验还表明，我们的检测系统优于现有两种工具（平均真正例率为96.7%，假正例率为0%）。

**关键词：**PowerShell；抽象语法树；混淆和解混淆；恶意脚本检测
https://doi.org/10.1631/FITEE.2000436