2011 XIX congresso interno de iniciação científica
CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico
UNICAMP

T0891

UMA FERRAMENTA INTERATIVA PARA VISUALIZAÇÃO DE COMPORTAMENTO DE PROGRAMAS MALICIOSOS

Alexandre Or Cansian Baruque (Bolsista PIBIC/CNPq) e Prof. Dr. André Ricardo Abed Grégio (Orientador), Centro de Tecnologia da Informação Renato Archer - CTI, MCT

Programas maliciosos (*malware*), tais como vírus e cavalos-de-tróia, são responsáveis por grande parte dos problemas de segurança em computadores e redes atualmente. Existem várias ferramentas para analisar exemplares de *malware*, as quais produzem relatórios textuais das atividades maliciosas executadas ou os encaixam em alguma categoria. Entretanto, a extração de informações destes relatórios pode ser difícil para um analista humano e a classificação pode ser errônea. Com a finalidade de facilitar a obtenção de dados úteis do comportamento de um *malware* independente de sua classificação e auxiliar na resposta a incidentes de segurança propõe-se, neste trabalho, uma ferramenta visual que permite a identificação de padrões comportamentais por parte do analista, de modo interativo. A ferramenta foi feita usando a linguagem de programação Java, juntamente com a biblioteca Java3D para criar os gráficos em três dimensões e possui uma interface que permite ao usuário explorar o comportamento do *malware* analisado (seleção, filtragem, rotação, etc.). Foram submetidos mais de 400 comportamentos de *malware* à ferramenta e puderam-se verificar padrões visuais que possibilitam o agrupamento daqueles cujas atividades são semelhantes, independente da classificação dada por mecanismos antivírus.

Visualização - Malware - Interativo