عنوان مقاله:
بهبود دقت تشخیص بدافزارها به کمک اطلاعات سرآیند و جدول بخش های فایل دودویی

محل انتشار:
کنفرانس بین المللی مهندسی و علوم کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
ناهید ملکی - *دانشکده مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران*

حمید رستگاری - *دانشکده مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران*

مهدی باطنی - *گروه مهندسی کامپیوتر و فناوری اطلاعات دانشگاه شیخ بهایی، اصفهان، ایران*

خلاصه مقاله:
بدافزارها به مجموعه برنامه هایی اطلاق می شود که قصد آسیب رساندن یا سرقت اطلاعات در یک سیستم کامپیوتری را داشته باشند. اینمجموعه برنامه ها به عنوان تهدیدی در برابر سیستم های اطلاعاتی به شمار می روند. امروزه با وجود روشهای تغییر شکل و پنهان سازی،شناسایی بدافزارها مشکل تر شده است. در حال حاضر، روشی که در ضد ویروس های تجاری مورد استفاده قرار می گیرد، روش مبتنی برامضاء می باشد که این روش قادر به شناسایی بدافزارهای جدید نمیباشد. در این پژوهش، یک روش تشخیص بدافزار بر اساس استخراجاطلاعات سرآیند PE و جدول بخش های فایل های دودویی ارایه شده است. از مجموعه فایل های آموزشی، اطلاعات سرآیند PE و جدول بخشها استخراج شده و در پایگاه داده ویژگی ها ذخیره می شوند. سپس فایل های آزمایشی با استفاده از دسته بندهای K نزدیکترین همسایه، ماشین بردار پشتیبان، بیزین، درخت تصمیم و شبکه عصبی در Rapidminer مورد بررسی قرار گرفتند. بطور میانگین دقت دسته بندها 98.51 % می باشد. همچنین برای کلیه دسته بندها نرخ تشخیص اشتباه نسبت به کارهای مشابه بهبود داشته است.

کلمات کلیدی:
تشخیص بدافزار، سرآیند PE، جدول بخش، طبقه بندی