عنوان مقاله:
ارایه یک سیستم تشخیص بدافزار مبتنی برتحلیل پویا با بهره گیری از تعامل با کاربر

محل انتشار:
کنفرانس ملی فناوری اطلاعات و جهاد اقتصادی (سال: 1390)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمدرضا قاسمی - *دانشجوی کارشناسی ارشد دانشگاه آزاد نجف آباد*

منصور امینی لاری - *دانشگاه آزاد اسلامی واحد علوم و تحقیقات فارس*

خلاصه مقاله:
امروزه بدافزارها با استفاده ازتکنیکهای مبهم سازی پیچیده تر شده اند و تشخیص آنها نیز دشوار گردیده است از این رو تلاش ها برای تشخیص بدافزارها چندریختی جدید و ناشناخته مارا به سمت طراحی سیستمی پویا جهت شناسایی بدافزارها هدایت م یکند دراین مقاله روشی برای ساخت یک پایگاه دادگان مناسب جهت تشخیص و شناسایی بدافزارهای ناشناخته به همراه روشی کارا برای ساخت و انتخاب بردارهای ویژگی پیشنهاد شده است سپس روشی مبتنی برروش دسته بندی ماشین بردار پشتیبان فازی به همراه معیاری مناسب برای فازی سازی میزان تعلق دادگان به دسته های مختلف جهت شناسایی بدافزارهای جدید پیشنهاد شده است درروش پیشنهادی از اطلاعات و نظر کاربرد در مورد موارد شناسایی شده نظر سنجی صورت می گیرد از این اطلاعات جهت تصحیح اشتباه های گذشته و افزایش یادگیری و تطبیق پذیری سیستم نسبت به بدافزارهای جدید و ناشناخته استفاده می شود درآزمایشات کارایی پایگاه دادگان و همچنین روش تشخیص پیشنهادی مورد ارزیابی قرارگرفت.

کلمات کلیدی:
بدافزار، تشخیص پویا، بدافزارهای چندریختی، دسته بندی کننده ماشین بردار پشتیبان فازی، تعامل با کاربر