عنوان مقاله:
شناسایی بدافزار با داده کاوی

محل انتشار:
پانزدهمین کنفرانس کامپیوتر سالانه انجمن کامپیوتر ایران (سال: 1388)

تعداد صفحات اصل مقاله: 8

نویسندگان:
حسین رحیمی - *دانشکده مهندسی برق و کامپیوتر؛ دانشگاه شیراز*

بابک یادگاری - *دانشکده مهندسی برق و کامپیوتر؛ دانشگاه شیراز*

اشکان سامی - *دانشکده مهندسی برق و کامپیوتر؛ دانشگاه شیراز*

ناصر پیرویان - *محقق شرکت نرم افزاری GCS*

خلاصه مقاله:
ظهور گسترده بد افزار به عنوان وسیله ای برای جرائم اینترنتی و ناتوانی روش های قدیمی ضد بدافزار در مقابل جریان پیوسته تولید انواع ناشناخته و تراریخته آن، رقابتی دائم را در زمینه مبارزه با این پدیده ایجاد نموده است. از این رو پژوهشهای اخیر درحال گام برداشتن به سوی شناخت بدافزار با استفاده از مشخصات غیرقابل تغییر آن هستند.در روش های متداول کنونی برای شناخت بد افزار ها از روشهای مقایسه الگوهایی که در فایل اجرایی بد افزار موجود است با پایگاه داده نرم افزار ضد بد افزار استفاده می شود. که این نوع شناسایی برای بد افزار های که به صورت پویا فایل اجرایی خود را تغییر می دهند مناسب نیستند. ما روش جدیدی برای ردیابی بدافزار با استفاده از اطلاعات موجود در سرآیند فایلهای اجرایی قابل حمل ویندوز معرفی کرده ایم که در صورت هر گونه تغییر در فایل اجرایی بد افزار قابل شناسایی است. روش ما ابتدا توابع رابط برنامه نویسی استفاده شده توسط هر فایل اجرایی را از سرآیند فایل خوانده ، سپس شاخص های جداکننده و مرتبط با دامنه پژوهش را استخراج می نماید و از این شاخص ها برای کلاس بندی بدافزار نا شناخته استفاده می کند . در صورت تغییر در فایل اجرایی فقط ترتیب شناسه ها عوض میشود که بر روی مدل ساخته شده تاثیری ندارد . آزمایش های انجام شده بر روی تعداد زیادی بدافزار و برنامه های بی ضرر نشان دهنده برتری این روش نسبت به روش های گذشته بوده، بطوریکه این تکنیک بر اساس سه فاکتور نرخ رهگیری ، میزان هشدار های نادرست و دقت کلاس بندی از پژوهشهای دیگر پیشی گرفته است.

کلمات کلیدی:
بد افزار، داده کاوی، فراخوانی API، انتخاب خصیصه ها، دسته بندی