عنوان مقاله:
تشخیص بدافزار به کمک داده کاوی برای بدافزارهای با توانایی دگردیسی

محل انتشار:
پنجمین کنفرانس بین المللی مهندسی برق و کامپیوتر با تاکید بر دانش بومی (سال: 1396)

تعداد صفحات اصل مقاله: 6

نویسندگان:
وحید کشوری - *کارشناس فناوری و اطلاعات*

وحید صفری - *کارشناس کامپیوتر گرایش فناوری اطلاعات*

خلاصه مقاله:
به موازات تکامل نرم افزارهای خوش خیم، توسعه دهندگان آن ، اقدامات امنیتی را پیاده سازی می کنند تا مطمین شوند محصولاتشان از امنیت بالایی برخوردار است .با کامل شدن این نرم افزارها، نویسندگان مخرب ها نیز سعی دارند تا با استفاده از تکنیک های چندریختی ، مبهم سازی ، دگردیسی و ...بدافزارهای به روزتری را تولید کنند که در دام ضد بدافزارها قرار نگیرد. اساس و پایه ی روش های قدیمی برای تشخیص مخرب ها، استفاده از روش مبتنی بر امضا است که در این روش ها، قسمتی از بدافزار به عنوان یک امضا برای آن در نظر گرفته می شود و بدافزار توسط همین امضا ,شناسایی و تشخیص داده می شود .این امضاها در داخل یک پایگاه داده ذخیره می شوند. به دلیل عدم موفقیت روش های قدیمی در تشخیص و شناسایی بدافزارهای جدید و ناشناخته، درسال های اخیر محققان تلاش کرده اند تا با استفاده از بعضی ویژگی های تغییر ناپذیر بدافزارها، روش های مطمین تری را برای تشخیص آنها ارایه دهند .نتایج به دست آمده نشان می دهد که روش های جدید دارای نرخ بالاتر تشخیص نسبت به روش های قدیمی تر هستند.در این مقاله قصد داریم روشی را برای تحلیل و دسته بندی فایل های قابل اجرا ارایه دهیم. روشی که ارایه شده است، تکنیک های داده کاوی را استفاده می کند.

کلمات کلیدی:
داده کاوی ، بد افزار، دگردیسی فایل ها، یادگیری شناسایی