سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
روشی برای کلاسه بندی بدافزارها براساس هدر فایل با استفاده ازتصویر سازی

محل انتشار:
دومین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
ابراهیم سیاحی - *دانشجوی کارشناسی ارشد امنیت اطلاعات، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

علی حمزه - *دانشیار، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

خلاصه مقاله:
بدافزارها برنامه هایی هستند که با هدف خرابکاری در سیستم، سرقت اطلاعات و یا دیگر اقدامات مخرب ایجاد می شوند. روشهای مختلفی برای شناسایی و کلاسه بندی بدافزارها معرفی شده اند. در این مقاله، روشی برای کلاسهبندی بدافزارها براساس هدر آنها با استفاده از تکنیک های پردازش و کلاسه بندی تصاویر معرفی میشود. در کار انجام شده نتایج کلاسه بندی براساس هادر فایلها در مقایسه با کلاسه بندی براساس خود فایلها، نشان میدهد که بهبود قابل قبولی در دقت کلاسه بندی فایلهای مذکور حاصل میشود. در روش معرفی شده، ورودیهای استفاده شده برای مرحله کلاسه بندی، ویژگیهایی هستند که از تصاویر حاصل از فایلها بدست می آیند و در این مرحله از روشهای یادگیری ماشین برای کلاسه بندی استفاده میشود

کلمات کلیدی:
بدافزار، کلاسهبندی، هدرفایل،Gist، KNN، SVM

لینک ثابت مقاله در پایگاه سیویلیکا:
https://civilica.com/doc/691451