عنوان مقاله:
مقایسه انواع روشهای شناسایی بدافزاربا استفاده از الگوریتم های داده کاوی

محل انتشار:
دومین همایش کامپیوتر، برق و فناوری اطلاعات (سال: 1391)

تعداد صفحات اصل مقاله: 7

نویسندگان:
زینب مسچی - *کارشناسی ارشد دانشگاه آزاد اسلامی واحد زنجان*

سیدمحسن هاشمی - *مدیرگروه تحصیلات تکمیلی مهندسی نرم افزار وهوش مصنوعی دانشگاه آزاد و*

خلاصه مقاله:
حجم بسیارزیاد بدافزارها و افزایش روزافزون آنها باعث بروز تهدیدات درنقاط امنیتی و اطلاعاتی شده است به گونه ای که دربسیاری ازکشورها مراکز دفاع سایبری از اهمیت بالایی برخوردار است درواقع فضای مجازی مانند مرزهای کشور اهمیت دارد همانطور که مرزهای کشور از جهت های مختلف مانند حمله های خارجی قاچاق مواد سارقان و .... مورد هجوم واقع می شود فضای مجازی نیز از اینگونه حملات درامان نیست و حتی بیشتر هم مورد هجوم واقع می شود تجربه نشان میدهد که بیشترین حمله ها از جانب بدافزارها بوده است برای شناسایی این نوع نرم افزارهای مخرب قبل از بروز اثرات تخریبی باید روشهایی برای شناسایی رفتارنرم افزارهای خوب و بد داشت تا تشخیص دهیم کدام مشکل زا است و کدام نیست برای این کارباید هردو گونه نرم افزار را بررسی کنیم تادر شناسایی خود دچار مشکل نهشویم دراین مقاله این رفتارها را جمع آوری کرده و برروی انها الگوریتم های داده کاوی را اعمال می کنیم و سعی می کنیم قابلیت های روش را بیان نموده و آن ها را با هم مقایسه کنیم.

کلمات کلیدی:
اسمبلی - بدافزار - PE-Miner N-Gram API Call.