عنوان مقاله:
مروری بر روش های تشخیص نفوذ بدافزارها با تکنیک های داده کاوی

محل انتشار:
چهارمین کنفرانس بین المللی پژوهش های کاربردی درمهندسی کامپیوتر و پردازش سیگنال (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
شقایق سیاهوشی - *دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، موسسه آموزش عالی هاتف، زاهدان*

امیر رجایی - *عضو هیات علمی گروه مهندسی کامپیوتر، دانشگاه ولآیت، ایرانشهر*

خلاصه مقاله:
امروزه سیستم های کامپیوتری هدف حملات نرم افزار های مخربی که ناخواسته وارد سیستم شدهاند و امنیت اطلاعات وکارکرد سیستم را به خطر میاندازند، قرار میگیرند که به آنها بدافزار میگویند. جهت شناسایی آنها از دو تکنیک عمدهتشخیص مبتنی بر امضا و مبتنی بر رفتار میباشد که به صورت تجزیه و تحلیل پویا و ایستا صورت میپذیرد. با توجه به اینکه بدافزارهای جدید از تکنیک های جدید و ترکیبی جهت پنهان سازی خود استفاده میشود، روش های سنتی قادر بهشناسایی آنها نبوده و امروزه از روشهای هوشمند مانند داده کاوی برای تشخیص نفوذ آنها استفاده میگردد. در این مقاله سعی شده بر مفاهیم کلی مروری داشته باشیم و به بررسی روش های تشخیص با استفاده از داده کاوی بپردازیم

کلمات کلیدی:
بدافزار، دادهکاوی، تشخیص بدافزار، تجزیه و تحلیل بدافزار