عنوان مقاله:
به تصویر کشیدن بدافزار و شناسایی بدافزارهای هم خانواده با استفاده از تکنیک تجزیه وتحلیل بافت دودویی

محل انتشار:
سومین کنفرانس ملی فناوری در مهندسی برق و کامپیوتر (سال: 1397)

تعداد صفحات اصل مقاله: 20

نویسنده:
امین مهدیزاده - *کارشناسی ارشد، فارغ التحصیل رشته مهندسی کامپیوتر- نرم افزار*

خلاصه مقاله:
امروزه بحث امنیت اطلاعات یکی از موضوعات اساسی در دنیای امروزی است و با توجه به رشد روز به روز بدافزارها چالشهای امنیتی به وجود آمده است و مورد توجه بسیاری از افرادی که در این زمینه فعالیت میکنند واقع شده است و همین امر ما را ملزم به یادگیری و آموزش در زمینه امنیت میکند.در این مقاله یک رویکرد جدیدی در زمینه امنیت ارایه میکنیم که روند کار به این صورت میباشد که، از بدافزارها تصویر برداری صورت میگیرد که این کار مستلزم استفاده از محتوای بدافزارها می باشد. محتوای بدافزارها را به صورت باینری ایجاد کرده سپس از طریق این کدهای باینری، بدافزار را به تصویر میکشیم و زمانیکه تصویر بدافزار را تولید کردیم میبایست بدافزار را شناسایی کنیم و متوجه بشیم اسم بدافزار چیست و مربوط به کدام خانواده از بدافزارها میباشد برای این کار از تصویر بدافزاری که در اختیار داریم با استفاده از تکنیک بافت تصویر، یکسری عملیات را بر روی تصویر بدافزار انجام میدهیم و زمانیکه عملیات بافت به سرانجام رسید باید یکسری خصوصیات از بدافزارها استخراج شود که این خصوصیات با استفاده از روشهای آماری بدست میآید و بر اساس این خصوصیات بدافزارهای مختلفی را پس از تجزیه و تحلیل، شناسایی کنیم.

کلمات کلیدی:
بدافزار، امنیت، باینری بدافزاری، ماتریس هم رخداد سطح خاکستری، پردازش تصویر، شناسایی