عنوان مقاله:
طراحی و پیاده سازی موتور دگردیسی بدافزارها با رویکرد ارزیابی کارایی روش های شناسایی

محل انتشار:
فصلنامه علوم و فناوری های پدافند نوین, دوره 4, شماره 3 (سال: 1392)

تعداد صفحات اصل مقاله: 11

نویسندگان:
مهران خسروی - *دانشگاه آزاد اسلامی، واحد بروجرد*

سعید پارسا - *دانشگاه علم و صنعت ایران*

خلاصه مقاله:
یکی از اصول پدافند غیر عامل مقاوم سازی سامانه ها در مقابل حملات است. دسته بزرگی از حملات از طریق حمله بدافزارها به سیستم های کامپیوتری صورت می گیرد. باید میزان کارایی روش های موجود در مقابله با حملات بدافزارها مورد ارزیابی قرار بگیرند. یکی از رویکردها در این زمینه انجام حملات مدیریت شده توسط بدافزارهای تولید شده با موتورهای هوشمند است. اکثر محصولات ضد بدافزار از روش های شناسایی مبتنی بر امضای کد دودویی برای شناسایی بدافزارها استفاده می کنند. خانواده ای از بدافزارهای کامپیوتری به نام بدافزارهای دگردیس وجود دارد که در هر نسل امضای خود را با بهره گیری از روش های مبهم سازی تغییر می دهند. بنابراین با این روش مانع از تشخیص توسط روش های شناسایی مبتنی بر امضا دودویی بدافزار می شوند. در این مقاله موتور دگردیسی مبتنی بر اتوماتای سلولی یادگیر طراحی شده است که به دلیل ماهیت پویای آن علاوه بر توانایی مقابله با روش های شناسایی مبتنی بر امضای دودویی کد، به دلیل ایجاد کدهای مشابه برنامه های بی خطر با درصد تشابه بالا، قابلیت مقابله با روش های شناسایی مبتنی بر تحلیل آماری کدها را نیز دارد. این موتور می تواند ابزاری مناسب جهت بررسی کارایی سیستم های موجود در مقابله با حملات احتمالی باشد.

کلمات کلیدی:
بدافزار دگردیس, امضای بدافزار, تحلیل آماری کد, موتور دگردیسی, مبهم سازی, اتوماتای سلولی یادگیر