عنوان مقاله:
ارائهی روشی برای تشخیص فراخوانیهای سیستمی محلی در بهبود دقت تشخیص بدافزارهای فشردهشده

محل انتشار:
کنفرانس بین المللی یافته های نوین پژوهشی درمهندسی برق و علوم کامپیوتر (سال: 1394)

تعداد صفحات اصل مقاله: 14

نویسندگان:
محمدرضا اخلاقی - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه شیخ بهائی، اصفهان.*

مهدی باطنی - *دکتری مهندسی کامپیوتر، دانشگاه شیخ بهائی، اصفهان.*

خلاصه مقاله:
امروزه بیشتر نرمافزارهای شناسایی بدافزار مبتنی بر امضا میباشند که در آنها توانایی شناسایی انواع مختلف یک بدافزار بهعنوان یک ویژگی مهم محسوب میگردد که این امر با شناسایی ویژگیهای ثابتی در نمونههای مرتبط امکانپذیراست. فراخوانیهای محلی روشی بدون واسطه، برای فراخوانی توابع سیستمی است. این مقاله برای شناسایی انواع مختلف یک بدافزار فشردهشده و چندریخت، روشی را معرفی میکند که در این روش از یک شبیهساز سطح برنامه، جهت خارجساختن فایل دودویی از حالت فشردهشده به حالت اولیهی بدافزار، و یک برنامه جهت تولید امضای توابع محلی به همراهشناسایی و تولید امضای بلوکهای موجود در فایل باینری استفاده میکند. علاوه بر این از یک الگوریتم جهت اندازهگیری تفاوت بین دو امضای مختلف، استفادهشده است. نوآوری این روش شناسایی فراخوانیهای محلی بهصورت ایستا میباشد.تمامی اطلاعات جمعآوریشده از بدافزار به همراه امضا و تفاوت آن با بقیه امضاهای موجود، در یک دیتاست ذخیرهشده و از آن در جهت استخراج نتایج استفاده میشود. در این پژوهش از ترکیبی از بدافزارهای واقعی برای نمایش دقت و کارایی روش ارائه شده، استفاده شده است، مجموعه بدافزارهای مورداستفاده شاملRoron و Klez، Netsky میباشد. نتایج به دست آمده به طور میانگین بین سه مجموعه بدافزار مورد مطالعه، 71.8 % نسب به کار قبلی، بهبود نشان میدهد

کلمات کلیدی:
بدافزار فشرده Packed Malware ، شبیهساز Simulator ، امضا Signature ، فراخوانی محلی Native Call