عنوان مقاله:
بررسی چند روش کشف رفتاری بدافزار مبتنی بر فراخوانی های سیستمی

محل انتشار:
اولین همایش منطقه ای شبکه های کامپیوتری (سال: 1392)

تعداد صفحات اصل مقاله: 8

نویسندگان:
سعید پارسا - *دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران*

مریم درخشانکار - *دانشجوی کارشناسی ارشد نرم افزار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران*

خلاصه مقاله:
به دلیل گسترش نرم‌افزارها و شیوه‌های مبهم‌سازی، امروزه تعداد بدافزارها رو به افزایش است، که یکی از مهم‌ترین تهدیدات سیستم‌های کامپیوتری محسوب می‌شود. بنابراین روش‌های تحلیل و تشخیص بدافزار پیشنهاد می‌گردند، که عمدتاً بر دو دسته کلی ایستا بر پایه تحلیل مبتنی بر امضا و پویا براساس تحلیل مبتنی بر رفتار تقسیم می‌شوند و گاهی هم ترکیبی از هر دو جنبه می‌باشد. به علت حجم زیاد بدافزارها تشخیص رد پای آن‌ها از طریق روش‌های تحلیل مبتنی بر امضا نمی‌تواند کافی باشد، از این رو محققان در پی روش‌های نوین موثرتر در زمینه حفاظت و امنیت که اغلب روش‌های تحلیل مبتنی بر رفتار (یا تلفیقی از امضا و رفتار) می‌باشند، تمرکز کرده‌اند. در زمینه تشخیص بدافزار در تحلیل مبتنی بر رفتار به طور کلی سه مشکل اساسی وجود دارد: عدم بررسی یک برنامه در حال اجرای آن، عدم استفاده از برنامه‌های سالم جهت ساخت مدل رفتارهای بدانیش و هم‌چنین سربار بالای این روش‌ها از لحاظ پیچیدگی زمانی مدل‌ها، هر کدام این مشکلات راهکارهایی را می‌طلبد. بررسی نرم‌افزار جهت کشف سالم یا بدانیش بودن، در حین اجرای آن صورت نمی‌گیرد، پس برای جلوگیری از آسیب به سیستم عامل باید فرآیند بررسی در محیط مجازی انجام شود، نه واقعی. از طرفی باید علاوه بر رفتار سوء یک بدافزار، کلیه رفتارهای آن مورد مطالعه قرار گیرد تا مدلی جامع تدارک دیده شود؛ و در نهایت تحلیل براساس بررسی گراف، درخت و خوشه‌بندی، سربار زمانی بالای دارد و باید تا حد امکان این امر نیز بهینه انجام شود.

کلمات کلیدی:
مبهم سازی، بدافزار، رفتار، تحلیل پویا