عنوان مقاله:
تحلیل و شناسایی بدافزارها با استفاده از داد کاوی و مهندسی معکوس

محل انتشار:
کنفرانس ملی فن آوری، انرژی و داده با رویکرد مهندسی برق و کامپیوتر (سال: 1394)

تعداد صفحات اصل مقاله: 8

نویسندگان:
سعید غلامی گرمیانه - *گروه مهندسی کامپیوتر واحد کرمانشاه دانشگاه آزاد اسلامی کرمانشاه ایران گروه مهندسی کامپیوتر واحد علوم و تحقیقات کرمانشاه دانشگاه آزاد اسلام*

علی حنانی - *گروه مهندسی کامپیوتر واحد کرمانشاه دانشگاه آزاد اسلامی کرمانشاه ایران گروه مهندسی کامپیوتر مرکزسنقر وکلیایی دانشگاه آزاد اسلامی سنقروکلی*

فرهاد مردوخی - *گروه مهندسی کامپیوتر واحد کرمانشاه دانشگاه آزاد اسلامی کرمانشاه ایران گروه مهندسی کامپیوتر وفناوری اطلاعات دانشکده فنی مهندسی دانشگاه راز*

خلاصه مقاله:
بدافزارها به قطعه کدهای مخربی اطلاق میگردند که از مهمترین و درعین حال جدیترین تهدیدات امنیتی برای سیستمهای کامپیوتری به شمار می روند . تعداد و تنوع آن یها عل رغم ارائهی راههای دفاعی متعدد، به موازات رشد فزاینده ی فضای سایبر آثار تخریبی فراوانی داشته اند که علت آن را میتوان اعمالی همچون مبهم سازی، رمزگذاری، بسته بندی و چندریختی برای گریز از شناسایی توسط ابزارهای ضد بدافزار و تولید کدهای پویای پنهان از دید کاربر دانست. بدافزارهای پیشرفته که با اهداف کلان به قصد جاسوسی و آسیب به زیرساختهای مهم و حیاتی یک کشور سازمان دهی و عملیاتی میگردند، ابزار بازگشایی آن حتی با پرداخت هزینههای هنگفت هم ارائه و یافت نمیگردد، بنابراین تحلیل و شناسایی بدافزارها به منظور پیشگیری و مقابله با اثرا ت جبران ناپذیر آن در پدافند غیرعامل از اهمیت بسزایی برخودار است. ما در این تحقیق قصد داریم رفتار بدافزار ها را با استفاده از دادهکاوی در حالت پویا تشخیص دهیم و با استفاده از تکنیکهای مهندسی معکوس رفتار آنها تحلیل نماییم . رفتار هر بدافزار می تواند دستورات اسمبلی، فراخوانهای سیستمی یا میزان تأثیر در حافظه باشد. در این راستا چارچوب و روشی جدید برای تحلیل و شناسایی آنها مطرح میگردد که بیانگر دقت بالا و نرخ صحیح تشخیص بدافزارها می باشد

کلمات کلیدی:
بدافزار، دادهکاوی، مهندسی معکوس، فراخوان سیستمی