عنوان مقاله:
تشخیص فعالیتهای سطح بالای حملات سایبری پیشرفته مبتنی بر پردازش زبان طبیعی

محل انتشار:
دومین کنفرانس بین المللی پژوهش های دانش بنیان در مهندسی کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 13

نویسندگان:
مرجان خیرخواه - *دانشجوی کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، تهران، ایران*

کوروش داداش تباراحمدی - *استادیار دانشگاه صنعتی مالک اشتر، تهران، ایران*

علی جباررشیدی - *دانشیار دانشگاه صنعتی مالک اشتر، تهران، ایران*

خلاصه مقاله:
تهدیدات APT، رشته حملات پیچیده و ماندگار نفوذ به شبکه بوده که شامل مراحل نامحسوس و مخفی متعددی از فعالیت های سایبری بدخواهانه می باشند. این نوع حملات توانایی ناشناخته ماندن را دارند، خود را در ترافیک شبکه سازمانی پنهان می کنند و فقط به قدر کافی برای دستیابی به اهداف تعیین شده فعل و انفعال دارند. یکی از دلایل ناکارامدی سیستم های تشخیص نفوذ فعلی در برابر APT ها، استفاده از مکانیزم دفاعی مبتنی بر آنالیز ترافیک شبکه ای سطح پایین است، در حالی که از اطلاعات ساختاری پنهان در داده های ترافیکی خام غافل مانده اند. فرض ما این است که در بطن ترافیک شبکه ای قواعدی مانند قواعد زبانی وجود دارند و می توان روش های زبانی را برای توصیف الگوهای فعالیت های شبکه ای بدخواهانه به کار گرفت و مساله کشف الگوهای سوء استفاده و ناهنجاری را همانند مساله یادگیری ساختارهای نحوی و قطعات مفهومی زبان شبکه حل کرد. با توجه به این که تا کنون تعداد بسیار اندکی از روش های مبتنی بر زبان برای کشف نفوذ شبکه پیشنهاد شده است، ما سعی کردیم از مفاهیم NLP و القای قواعد زبان طبیعی برای کشف الگوهای فعالیت های سطح بالای شبکه استفاده کنیم. در ضمن در بخشی از این کار در ادغام رفتاهای سطح پایین با استفاده از خوشه بندی سلسله مراتبی، از چند معیار شباهت استفاده کرده ایم که در این میان معیار شباهت فاصله ویرایش برای اولین بار در این حوزه استفاده شده است. نتایج نشان می دهد دقت تشخیص در این روش نسبت به روش های پیشین ..... بهبود داشته است.

کلمات کلیدی:
حملات ماندگار پیشرفته ، تشخیص حملات سایبری، پردازش زبان طبیعی، معناشناسی