عنوان مقاله:
ارائه روشی نوین جهت شناسایی بات نت ها در شبکه مبتنی بر زنجیره مارکوف

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 9, شماره 3 (سال: 1400)

تعداد صفحات اصل مقاله: 14

نویسندگان:
عزیز عزت نشان - *گروه مهندسی کامپیوتر، واحدنیشابور، دانشگاه آزاد اسلامی، نیشابور، ایران*

سیدرضا کامل طباخ فریضنی - *گروه مهندسی کامپیوتر، واحدمشهد، دانشگاه آزاد اسلامی، مشهد، ایران*

مریم خیرآبادی - *گروه مهندسی کامپیوتر، واحدنیشابور، دانشگاه آزاد اسلامی، نیشابور، ایران*

رضا قائمی - *گروه مهندسی کامپیوتر، واحد قوچان، دانشگاه آزاد اسلامی، قوچان، ایران*

خلاصه مقاله:
بات نت ها در حال حاضر طیف وسیعیاز حملات اینترنتی را تشکیلمی دهند. بات نت ها، شبکه ای از کامپیوترهای آلوده متصل به اینترنت، با کنترل از راه دور می باشند. تاکنون تحقیقات زیادی در این زمینهانجام شده است کهبر اساس امضاهاییات نت هایکشف شده، ناهنجاری ها، رفتار ترافیکی،آدرس هااست. این روش هاتاکنوننتوانسته اند نرخ کشف بالایی را داشته باشندمخصوصا برای بات نت هایی که در شرایط خاصی رفتار اصلی خود را بروز می دهند و یا این روش‌ها می‌بایست برای مقایسه گذشته بات را به طور کامل به خاطر بسپارند که این در مواردی نیازمند به حافظه بسیار بزرگی هست که در عمل غیرممکنمی شود. هدف از این تحقیق پیشنهاد ساختاری برای انجام عملیات شناسایی است که این کار در این تحقیق مبتنی بر زنجیره مارکوف ارائه شده است و سعی بر عدم استفاده از حافظه است. زنجیره مارکوف ارائه شده در این تحقیق نیازمند به حافظه نگهداری نیستو بر اساس تحلیل رفتاریمی باشد. روش پیشنهادی قادر است تا رفتارهاییات نت ها را با بررسیناحیه رفتاری، بهتر از راهکارهای گذشته بررسی نماید که بدین شکل نیازمند به بررسی کل جریان نیست بلکه نقاط خاصی بررسی می شوند که این باعث کاهش سربار محاسباتی می شود. در این تحقیقمعیارهای مختلفی همچونخطای میانگین مربعات، دقت و صحت موردبررسی قرار گرفت و در تمامی این موارد روش پیشنهادیبه صورتقابل ملاحظه ای بهتر از باقیروش های مورد مقایسه عمل نمود.

کلمات کلیدی:
زنجیره مارکوف, کشف بات نت, جریان شبکه, استخراج ویژگی