شناسایی بات نت ها با استفاده از تحلیل ترافیک DNS سرورها

مهرداد موسی خواه کوشالی *,دکتر رضا ابراهیمی آتانی,

1395-6-20

بات‌نت به گروهي از ماشين‌هاي آلوده شده در سطح شبکه گفته مي‌شود که از راه دور توسط مدير باتـ¬نت کنترل مي‌شوند. بات‌نت به زيرساخت ارتباطي به نام کانال کنترل و فرمان نياز دارد تا مدير بات بتواند از طريق آن فرامين خود را براي بات‌ها ارسال کند و پاسخ را دريافت کند. باتـ¬نتـ¬ها معمولاً براي هدايت انواع فعاليت‌هاي خرابکارانه مورد استفاده قرار مي‌گيرند. از اين جهت مقابله با آنها از اهميت بالايی برخوردار است. روشـ¬های متعددی جهت تشخيص باتـ¬نتـ¬ها به کار گرفته شده است که هر يک دارای معايب و مزايايی ميـ¬باشند. تلاش مديران بات برای فرار از اين روشـ¬های تشخيصی، باعث خلق روش-های جديد در باتـ¬نتـ¬ها شده است. در اين تحقيق روشی طراحی شده است که با استفاده از دادهـ¬کاوی نامـ¬های دامنه، دامنهـ¬های بد از دامنهـ¬های خوب شناسايی شود. روش پيشنهادی شامل خواندن دامنهـ¬های خوب از فايل، ايجاد دامنهـ¬های بد به صورت پويا و اضافه کردن تعدادی دامنه بد حقيقی، برچسب زدن خوب و بد دادهـ¬های آموزشی و مرحله آخر ايجاد طبقهـ¬بنديـ¬کننده با استفاده از الگوريتم بيز و ذخيره در فايل ميـ¬باشد. با پيادهـ¬سازی اين روش، نتايج حاصل در مقايسه با دو روش تشخيص باتـ¬نت به نامـ¬های Yadav و Pedro، کارآيی بهتری را ارائه داده و درصد درستی 99% را نشان ميـ¬دهد.

کلمات کليدی : باتـ¬نت، کانال فرمان‌وکنترل، ترافيک DNS سرورها، نام دامنه، دادهـ¬کاوی، الگوريتم بيز