عنوان مقاله:

شناسایی دامنه های بدخواه شبکه های بات با استفاده از شبکه عصبی خود رمزگذار عمیق DOR: ۲۰.۱۰۰۱.۱.۲۳۲۲۴۳۴۷.۱۴۰۰.۹.۱.۵.۲

محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری, دوره 9, شماره 1 (سال: 1400)

تعداد صفحات اصل مقاله: 14

نویسندگان:

مهدی اسدی – مربی، گروه مهندسی کامپیوتر، واحد خامنه، دانشگاه آزاد اسلامی، خامنه، ایران

سعید پارسا – دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران

وحید وثوقی – کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد شبستر، دانشگاه آزاد اسلامی، شبستر، ایران

خلاصه مقاله:

هر شبکه بات گروهی از میزبان هایی است که با کد بدخواه یکسانی آلوده شده و از طریق یک یا چند سرویس دهنده فرمان و کنترل توسط مهاجم یا مدیر بات هدایت می شوند. در شبکه های بات نسل جدید فهرست نام های دامنه سرویس دهنده‌های فرمان و کنترل به صورت پویا ایجاد می شود. این فهرست پویا که توسط یک الگوریتم تولید دامنه ایجاد می شود به مهاجم کمک می کند تا مکان سرویس دهنده‌های فرمان و کنترل خود را به صورت دوره ای تغییر داده و از قرار گرفتن آدرس های آن ها در فهرست های سیاه جلوگیری کند. هر میزبان آلوده با استفاده از یک الگوریتم از پیش تعریف شده، تعداد زیادی نام دامنه تولید کرده و با ارسال پرس وجوهای سرویس دهنده دامنه تلاش می کند آن ها را به آدرس های متناظرشان نگاشت کند. در این مقاله، از الگوریتم شبکه عصبی خود رمزگذار عمیق برای شناسایی دامنه‌هایی که هیچ گونه آگاهی از الگوریتم تولید آن ها وجود نداشته است، استفاده شده و عملکرد روش پیشنهادی با عملکرد الگوریتم‌های یادگیری ماشین مقایسه شده است. ابتدا مجموعه داده جدیدی از ترکیب یک مجموعه داده با دامنه‌های سالم و دو مجموعه داده حاوی دامنه‌های بدخواه و ناسالم ایجادشده و از دو سناریوی دستی و خودکار برای استخراج ویژگی‌های مجموعه داده جدید استفاده شده است. شبکه عصبی خود رمزگذار عمیق بر روی مجموعه داده جدید و پیش پردازش شده اعمال شده و نتایج در مقایسه با الگوریتم‌های یادگیری ماشین بررسی شده است. با توجه به نتایج به دست آمده، می‌توان با استفاده از شبکه عصبی خود رمزگذار عمیق، دامنه‌های بدخواه تولیدشده توسط الگوریتم‌های تولید دامنه را با سرعت بیشتر و نرخ صحت بیشتر از ۹۸.۶۱% شناسایی کرد.

کلمات کلیدی:

شبکه بات, الگوریتم های تولید دامنه, استخراج ویژگی, شبکه عصبی عمیق, شبکه عصبی خود رمزگذار عمیق

لینک ثابت مقاله در پایگاه سیویلیکا: