بررسی نحوه عملکرد باتنت‌های مبتنی بر کانال‌های پنهان

مینا صاحبی *

کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه آزاد قزوین

چکیده

امروزه باتنت‌ها یکی از مهم‌ترین تهدیدات در برابر زیرساخت اینترنت شناخته می‌شوند. هر باتنت گروهی از میزبان‌هایی است که با کد مخرب یکسانی آلوده‌شده و از طریق یک یا چند سرویس‌دهنده فرمان و کنترل توسط مهاجم از راه دور هدایت می‌شوند. همزمان با ارائه پیشنهادهای جدید برای شناسایی باتنت‌ها، مهاجمین از روش‌های مقاوم‌تری جهت عدم شناسایی باتنت خود استفاده می‌کنند. از آن‌جایی که با شناسایی کانال‌های فرمان و کنترل به آسانی می‌توان باتنت‌های مختلف را متلاشی کرد، شناسایی این کانال‌ها در روش‌های تشخیص باتنت از اهمیت زیادی برخوردار است. مهاجمین با هدف افزایش طول عمر باتنت‌های خود از استراتژی‌های متفاوتی برای ایجاد کانال‌های فرمان و کنترل استفاده می‌کنند. از این‌رو باتنت‌های مختلف با سازوکارهای مختلفی ایجاد شده‌اند. در این پژوهش سعی شده است که به بررسی انواع مختلف کانال‌های فرمان و کنترل در باتنت‌ها و روش‌های مختلفی که مهاجمان از آن برای کنترل باتنت‌های خود استفاده می‌کنند، پرداخته و روش‌های مختلفی را که برای تشخیص این نوع باتنت‌ها معرفی شده اند بیان شود.

کلمات کلیدی: باتنت، کانال فرمان و کنترل، کانال پنهان، تشخیص باتنت.

۱. مقدمه

با گسترش روزافزون شبکه‌های کامپیوتری و ازدیاد حجم اطلاعات مورد مبادله در آن‌ها، امنیت شبکه به یک چالش بزرگ برای مدیران شبکه تبدیل شده است. همزمان با سیر پیشرفت فن‌آوری اطلاعات و ارائه خدمات نوین اینترنتی توسط مؤسسات و شرکت‌های مختلف خصوصی و دولتی، مهاجمین نیز از عواملی چون ناآگاهی کاربران و آسیب‌پذیری‌های مختلف موجود در نرم‌افزارها سوءاستفاده کرده و مشکلاتی را برای کاربران ایجاد کرده‌اند. در حال حاضر امنیت در اینترنت با یک تحول و تکامل از انواع حملات مواجه شده است. همواره تکنیک‌های پیچیده و متفاوت زیادی توسط مهاجمین در بدافزارها استفاده می‌شود تا بتوانند از شناسایی شدن توسط سیستم‌های تشخیص نفوذ جلوگیری کنند. حملات اینترنتی با انگیزه‌های مختلفی از قبیل کسب شهرت و درآمد، سرگرمی، خراب‌کاری و اهداف سیاسی انجام می‌شوند. در چند سال گذشته، اهداف و جهت‌گیری این تهدیدات به طور قابل ملاحظه‌ای تغییر یافته و به سمت سازماندهی بهتر و سود محوری بیشتر تکامل پیدا کر ده‌اند [۱].یکی از مهم‌ترین ویژگی سرویس‌دهنده‌های اینترنتی دسترس‌پذیری همیشگی آن‌ها است. در صورت عدم

* **Email:mina.sahebi.one@gmail.com**