

## چکیده

سایتهای شبکه اجتماعی با تعداد زیاد کاربران و بانکه اطلاعاتی وسیع از آنان زمینه خوبی برای تحت تاثیر قراردادن افراد و فریب آنها به منظور مهندسی اجتماعی<sup>1</sup> می باشند. در این راستا هکرها هم این روزها از حملات قدرتمندتری استفاده می کنند. بات نت<sup>2</sup>ها نمونه ای از این نوع حملات هستند. بات نت ها مجموعه ای از ماشین های آلوده شده در سطح اینترنت می باشند که توسط مهاجمان برای انجام دادن فعالیت های بدخواهانه و غیرقانونی از راه دور کنترل می شوند. برای مقابله موثر با این بدافزارها نیازمند بررسی دقیق کانالهای فرمان و کنترل در آنها هستیم. بر خلاف کرمها و ویروسها که معمولا اهداف خرابکارانه دارند هدف از به کارگیری بات نت ها توسط کنترل کنندگان آنان معمولا مالی می باشد. با توسعه ی سریع سرویس های شبکه های اجتماعی و تنوع حملات مهندسی اجتماعی ، گروه جدیدی از بات نت ها با عنوان بات نت های شبکه های اجتماعی از حملات مهندسی اجتماعی برای گسترش بات ها در شبکه های اجتماعی استفاده می کنند. این مساله تبدیل به یکی از چالشهای بزرگ برای سیستمهای امنیتی در جهان شده است. زیرا مهاجمین به سرعت در حال تغییر استراتژی های خود برای کانالهای فرمان و کنترل هستند. تمرکز ما در این مقاله بر روی راهها و الگوریتم های شناسایی نفوذ بات نت ها در شبکه های اجتماعی و مقابله با آنها می باشد.

**واژگان کلیدی:** بات نت - روشهای تشخیص حمله - شبکه های اجتماعی - مهندسی اجتماعی

---

<sup>1</sup>.social engineering

<sup>2</sup>.botnet