سومین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی
گرجستان - تفلیس (۳۰ تیرماه ۱۳۹۸) آکادمی بین المللی علوم گرجستان
ICIRES 21 July 2019
www.icires.ir
info@icires.ir
CIU
NVU
Eco energy
GIAS

مکانیزم حملات فیشینگ و ویژگی حملات در سرقت اطلاعات

امیر زارع[۱]، کمال میرزائی[۲]
[۱]دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد میبد، گروه کامپیوتر، ایران، amir30nov1993@gmail.com
[۲] عضو هیات علمی، دانشگاه آزاد اسلامی، واحد میبد، گروه کامپیوتر، ایران، k.mirzaie@maybodiau.ac.ir

چکیده – یکی از چالش‌های مهم وب سرقت اطلاعات و فیشینگ است که اطلاعات مهم کاربران را مورد سرقت قرار می‌دهد. در حملات فیشینگ یک وب‌سایت جعلی به جای وب‌سایت قانونی به کاربران معرفی شده و از طریق روش‌های فریب کاربران به سمت صفحات جعلی که بسیار شبیه صفحات قانونی می‌باشند هدایت می‌شوند. صفحات فیشینگ زیان قابل توجه‌ای به کاربران وارد می‌نمایند از طرفی اعتماد کاربران را کاهش می‌دهند. حملات فیشینگ دارای مجموعه‌ای از ویژگی‌ها بوده که شناخت آنها می‌تواند برای مقابله با این حملات مفید باشد. در این مقاله رویکرد حملات برای سرقت اطلاعات و چرخه فیشینگ معرفی شده سپس تعدادی از ویژگی‌های حملات معرفی شده تا کاربران اینترنت با آگاهی از آنها کمتر در دام این حملات قرار گرفته شوند و در ادامه نیز از تعدادی از روش‌های مقابله با حملات فیشینگ و شناسایی صفحات جعلی در اینترنت با استفاده از روش‌های یادگیری ماشین یا اکتشافی ارایه شده است. نتایج پژوهش ما نشان می‌دهد حملات فیشینگ در حین سادگی انجام دارای زیان قابل توجه‌ای بوده و از طرفی این حملات در صدر حملات اینترنتی از نظر تعداد قرار دارد همچنین استفاده از روش‌های ترکیبی مانند یادگیری ماشین و الگوریتم‌های اکتشافی یک روش مناسب برای مقابله با این حملات است.

کلید واژه- فیشینگ، سرقت اطلاعات، حملات تحت وب، صفحات جعلی

۱-مقدمه

وب‌سایتهای جعلی[۱] یکی از مشکلات مهم در اینترنت به شمار می‌روند و این صفحات جعلی ظاهری بسیار شبیه به وب‌سایتهای قانونی[۲] دارند. در حملات فیشینگ یک سایت جعلی در اینترنت به کاربران به عنوان سایت قانونی معرفی شده و از کاربران با روش‌های مختلف فریب نظیر مهندسی اجتماعی[۳] و با ابزارهای مانند ایمیل خواسته می‌شود که وارد سایت مورد نظر شده و اطلاعات خود را وارد این صفحات جعلی نمود و فیشر یا هکر در فرصت مناسب این اطلاعات را مورد سرقت قرار دهد[۱].

در حملات فیشینگ یک چرخه وجود دارد که در ابتدا یک سایت به عنوان سایت جعلی خود را به جای سایت قانونی معرفی نموده سپس لینک‌های جعلی آن از طریق ایمیل برای کاربران ارسال می‌شود. کاربران با دریافت ایمیل می‌توانند بر روی لینکهای جعلی که شبیه لینکهای قانونی است کلیک نموده و ناخودآگاه و ناخواسته وارد صفحات جعلی در اینترنت می‌شوند و اطلاعات مهم آنها مورد سرقت قرار گرفته می‌شود[۲].

صفحات جعلی در اینترنت زیان قابل توجه‌ای به کاربران وارد نموده زیرا تعداد زیادی از این صفحات جعلی درگاه‌های پرداخت یا سایتهای فروش را هدف قرار می‌دهند و از این طریق اطلاعات مهم کاربران مانند کلمه و رمز عبور بانکی آنها را سرقت نموده و به آنها دستبرد مالی می‌زنند از این رو این حملات به کاربران و بخش‌های مالی اینترنت زیان قابل توجه‌ای وارد می‌نمایند. برآوردها نشان می‌دهند که بیشتر قربانیان فیشینگ کاربران سیستم پرداخت آنلاین می‌باشند که قصد پرداخت الکترونیک دارند لذا زیان مالی حملات مالی زیاد است[۳]. حملات فیشینگ و صفحات جعلی دارای مجموعه‌ای از رویکرد و ویژگی است که

[۱]Fake websites
[۲]Legal website
[۳]Social engineering