مرکز آموزش الکترونیکی دانشگاه علم و صنعت

روشهای تشخیص حملات فیشینگ و راههای مقابله با آنها

پایان‌نامه برای دریافت درجه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات

گرایش مخابرات امن

شکرالله شکری

استاد راهنما:

دکتر رضا برنگی

بهمن ماه ۱۳۹۰

چکیده

فیشینگ یک نوع حمله اینترنتی در سطح وب می باشد که هدف اساسی آن سرقت مشخصات فردی کاربران می‌باشد. در حمله فیشینگ مهاجم تلاش می‌کند اطلاعات حیاتی و محرمانه کاربران مانند نام کاربری، رمز عبور و شماره کارت اعتباری را با فریب دادن افراد از طریق تغییر قیافه دادن و ظاهر شدن به عنوان یک شخص یا شرکت معتبر در ارتباطات الکترونیکی بدست آورد. در حقیقت فیشینگ یک شکل از دزدی برخط می‌باشد که از طریق فریب دادن کاربران کامپیوترها و بدست آوردن اطلاعات شخصی آنها با استفاده از وب‌سایت جعلی اتفاق می‌افتد. فارمینگ یکی از گونه‌های پیشرفته حملات فیشینگ می‌باشد که از نقاط ضعف سرویس نام دامنه[1] برای تغییر جهت ترافیک یک سایت وب به سایتی دیگر سوء استفاده می‌کند. به عبارت دیگر فارمینگ یک حمله بر روی یک DNS سرور است که به فیشر امکان می‌دهد کاربران را از سایت واقعی به سایت جعلی هدایت نماید. تاکنون روشهای مختلفی برای مقابله با حملات فیشینگ ارائه شده‌اند اما هیچکدام از آنها نتوانسته‌اند این حمله را به صورت کامل متوقف سازند. در این پایان‌نامه ضمن مرور حملات فیشینگ و روشهای جلوگیری از آنها، راهکاری جهت مقابله با این حمله ارائه شده است که با ساز و کارهای کنونی دنیای وب هم‌خوانی داشته و بکارگیری آن نیازی به اعمال تغییرات گسترده در ابزارهای کنونی وب ندارد. در روش ارائه شده سعی بر این است تا با پوشش آسیب پذیری سرویس‌های نام دامنه، از دسترسی کاربران به سایت جعلی جلوگیری بعمل آورده تا بدین ترتیب با نوع جدید حملات فیشینگ موسوم به فارمینگ مقابله گردد. نتایج آزمونهای آماری نشان داده که این روش از نرخ موفقیت بسیار بالائی برخوردار بوده و در جلوگیری از حملات فارمینگ کارائی مناسبی داشته و تقریبا صد درصد حملات فارمینگ را به خوبی تشخیص می‌دهد.

کلمات کلیدی: فیشینگ، فارمینگ، سرقت اطلاعات، حملات اینترنتی، امنیت اطلاعات

[1] Domain Name Service(DNS)

فهرست مطالب

فصل اول: مقدمه

فصل دوم: شناخت حملات فیشینگ

فصل سوم: روشهای جلوگیری از حملات فیشینگ