بسمه تعالی

سوءاستفاده از مدیران گذرواژه بااستفاده از ردیاب‌های وب

اکثر مرورگرها دارای یک مدیر گذرواژه‌ی داخلی هستند. مدیر گذرواژه ابزاری جهت ذخیره‌سازی اطلاعات ورود در یک پایگاه داده و پرکردن فرم‌ها یا ورود خودکار به سایت‌ها با استفاده از اطلاعات موجود در همان پایگاه داده است.

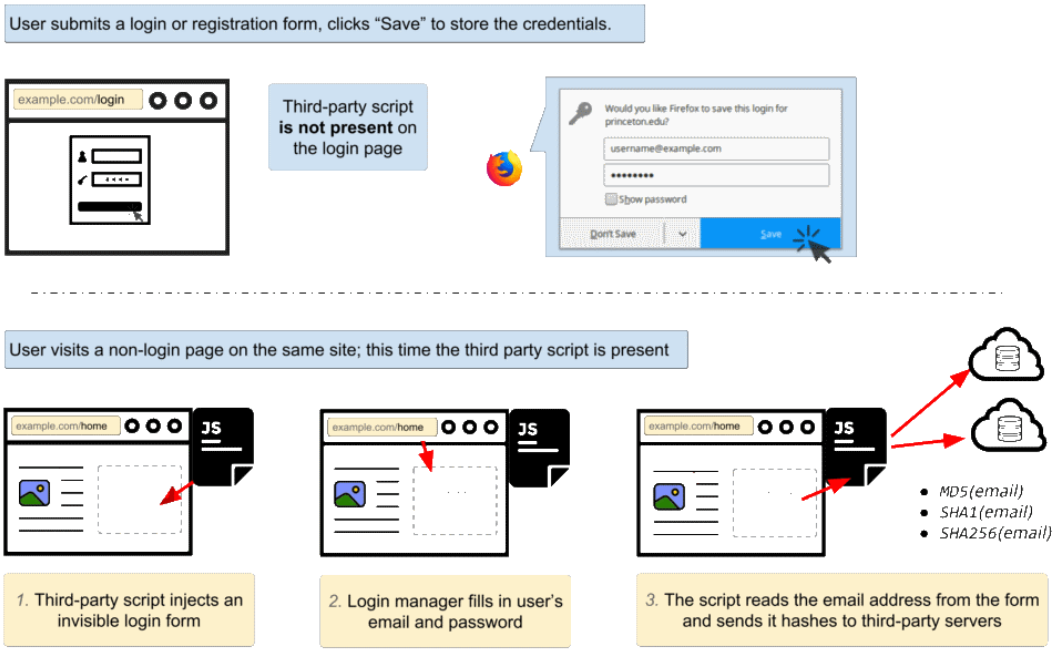
کاربرانی که قابلیت بیشتری می‌خواهند بر مدیران گذرواژه مانند LastPass، KeePass و DashLane تکیه می‌کنند. این مدیران گذرواژه قابلیت‌هایی را اضافه می‌کنند یا ممکن است به عنوان افزونه‌های مرورگر یا برنامه‌های میزکار نصب شوند.

تحقیقات مرکز Priceton نشان می‌دهد ردیاب‌های وبی که به‌تازگی کشف شده‌اند برای ردیابی کاربران از مدیران گذرواژه سوءاستفاده می‌کنند.

اسکریپت‌های ردیابی از ضعف مدیران گذرواژه سوءاستفاده می‌کنند. اتفاقی که می‌افتد به شرح زیر است:

- کاربر از یک وب‌سایت بازدید می‌کند، یک حساب کاربری ثبت می‌کند و اطلاعات را درمدیرگذرواژه ذخیره می‌سازد.
- اسکریپت ردیابی در پایگاه‌های وب شخص ثالث قرار داده شده و از طریق وب‌سایت اصلی اجرا می‌شود. وقتی کاربری از آن سایت بازدید می‌کند، فرم‌های ورود به سایت به صورت مخفیانه توسط اسکریپت ردیابی، در سایت تزریق می‌شوند.
- اگر سایت مطابقی در مدیر گذرواژه یافت شد، مدیر گذرواژه‌ی مرورگر اطلاعات را در آن پر خواهد کرد.
- اسکریپت ردیابی نام کاربری را شناسایی، آن را درهم‌سازی (hash) می‌کند و برای ردیابی کاربر به کارگزار شخص ثالث ارسال می‌کند.

شکل زیر روش کار را نشان می‌دهد:



محققان دو اسکریپت متفاوت را که برای سوءاستفاده از مدیران گذرواژه طراحی شده‌اند تا اطلاعات قابل شناسایی کاربران را دریافت نمایند، مورد تجزیه و تحلیل قرار داده‌اند. این دو اسکریپت AdThink و OnAudience نام دارند و فرم‌های ورود مخفی را در صفحات وب تزریق می‌کنند تا داده‌های نام کاربری را از مدیر گذرواژه‌ی مرورگر بازیابی نمایند.

این اسکریپت‌ها هش‌ها را محاسبه می‌کنند و آن‌ها را به کارگزار شخص ثالث ارسال می‌کنند. این هش برای ردیابی کاربران در سایت‌ها، بدون استفاده از کوکی‌ها و دیگر فرم‌های ردیابی کاربر استفاده می‌شود.

ردیابی کاربر برای تبلیغات آنلاین کارایی فراوانی دارد. شرکت‌ها از این اطلاعات برای ایجاد نمایه‌های کاربر که علایق کاربر را بر اساس تعدادی از عوامل، برای مثال بر اساس سایت‌های بازدیدشده (ورزش، سرگرمی، سیاسی، علمی) شناسایی می‌کند، استفاده می‌کنند.

محققان بیش از ۵۰۰۰۰ پایگاه وب را مورد تجزیه و تحلیل قرار داده‌اند و در هیچ یک از آن‌ها روبرداری از گذرواژه را مشاهده نکردند. آن‌ها اسکریپت‌های ردیابی را در ۱۱۰۰ پایگاه وب از ۱ میلیون پایگاه وب اول Alexa یافتند.

در این روش از اسکریپت‌های زیر استفاده شده است :

AdThink: https://static.audienceinsights.net/t.js

OnAudience: http://api.behavioralengine.com/scripts/be-init.js

جهت حفاظت در برابر ردیابی وب فرم ورود، کاربران می‌توانند مسدودکننده‌های محتوا را نصب کنند تا درخواست‌ها به دامنه‌هایی که به آن‌ها اشاره شده است را مسدود نمایند. روش دیگر غیرفعال‌سازی پرکردن خودکار داده‌های ورود به سایت است.