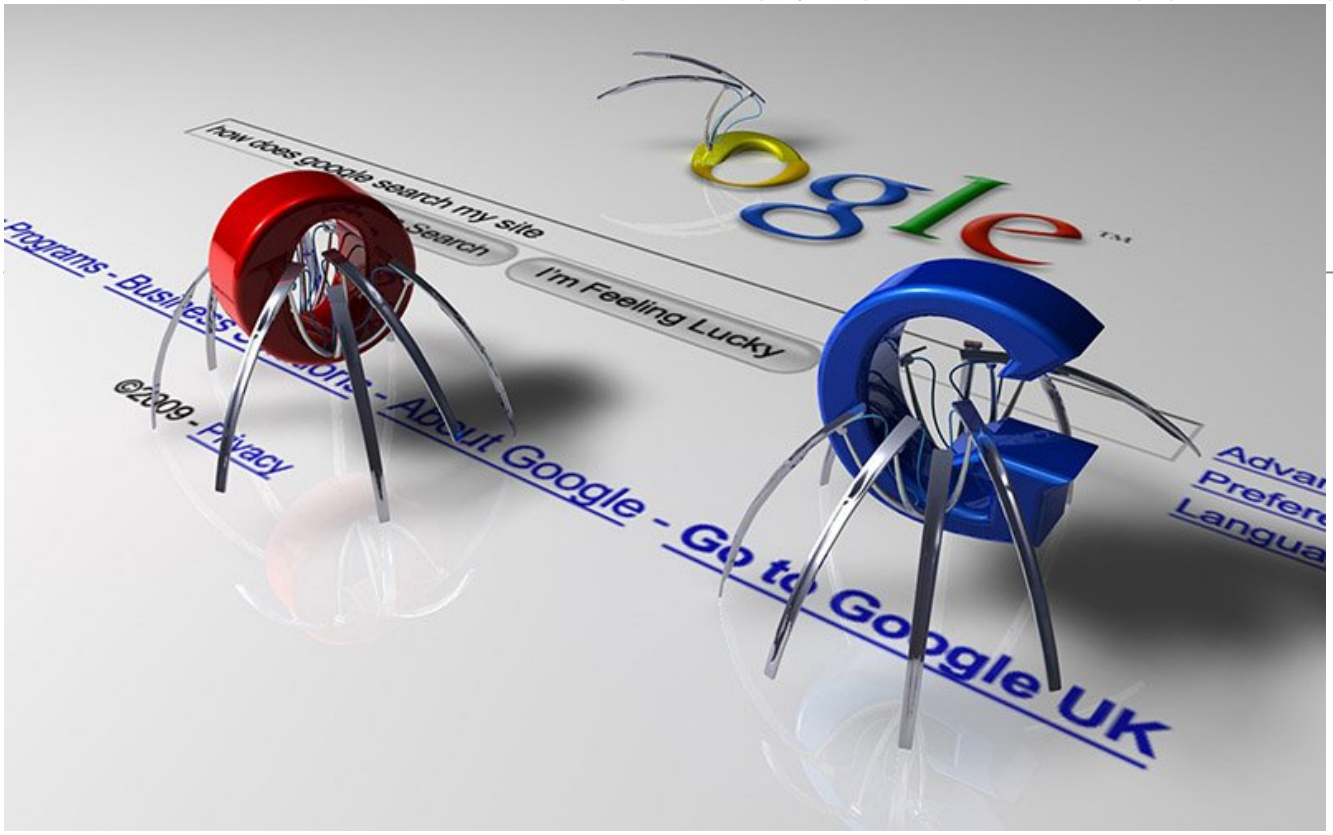
Malvertising در سال‌های اخیر به مشکل بزرگی تبدیل شده است

پرسه بدافزارهای تبلیغاتی در کمپین‌های گوگل



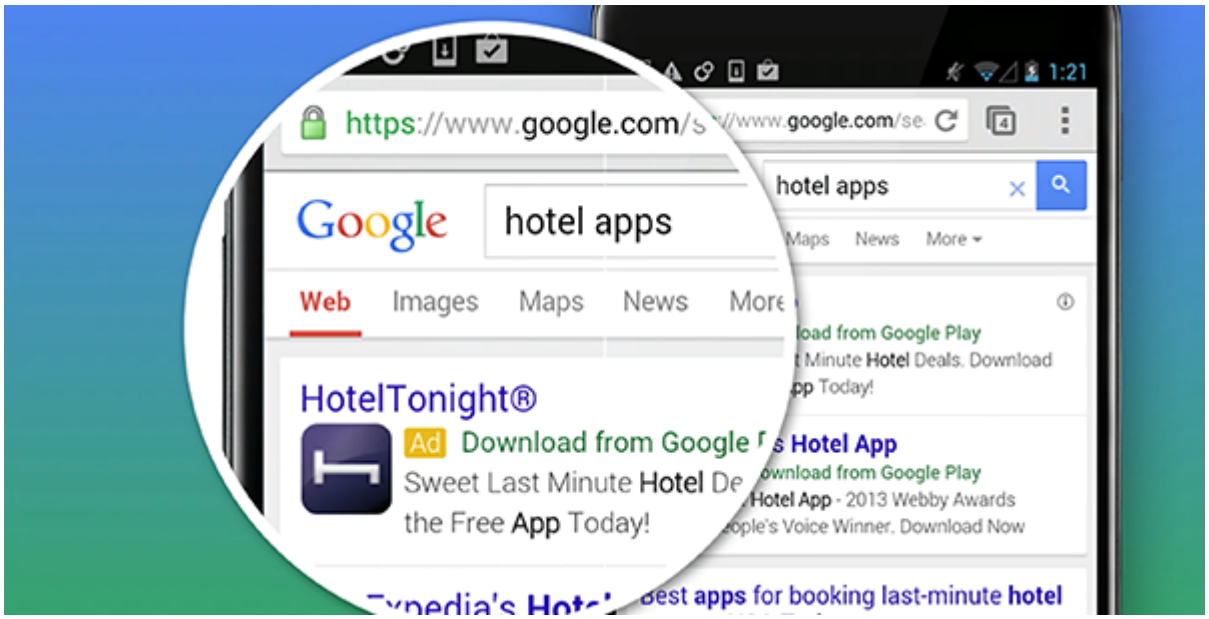
تعداد زیادی از تبلیغات توزیع شده توسط شرکت‌های تجاری همکار گوگل، کاربران را به سوی اکسپلویت‌های مبتنی بر وبی هدایت می‌کنند که سعی دارند بدافزارهایی را روی کامپیوترها نصب کنند.

محققان امنیتی از شرکت هلندی Fox-IT کمپین بدافزارهای تبلیغاتی راه‌اندازی شده توسط شرکت همکار گوگل در بلغارستان را زیر نظر گرفتند و متوجه شدند تمام کاربران را به سوی یک کیت اکسپلویت موسوم به کیت هسته‌ای هدایت می‌کند. کیت اکسپلویت یک پلتفرم حمله مبتنی بر وب است که سعی می‌کند آسیب‌پذیری‌های درون مرورگرهای وب و افزونه‌های آن‌ها را بیابد تا از این طریق بتواند نرم‌افزارهای مخرب و آلوده را روی کامپیوترهای قربانی نصب و اجرا کند.

Nuclear Exploit Kit به‌طور ویژه آسیب‌پذیری‌های نرم‌افزارهای ادوبی فلش پلیر، جاوای اوراکل و سیلورلایت مایکروسافت را هدف قرار داده است. یک محقق شرکت Fox-IT در وبلاگ خود گزارش می‌دهد: «به‌نظر می‌رسد تمام تبلیغات روی وب‌سایت engagelab.com به یک دامنه هدایت می‌شوند که ترافیک را به روی Nuclear Exploit Kit منتقل می‌کند. این کار حرکت شیطنت‌آمیز نمایندگی فروش سرویس‌های تبلیغاتی گوگل است.»

پس از این‌که ترافیک زیادی روی وب از این طریق به سوی این اکسپلویت هدایت شدند، ارجاع ترافیک‌ها از سایت engagelab به آن دامنه به‌طور کامل متوقف می‌شود که حکایت از مداخله گوگل یا مدیران خود سایت برای جلوگیری از دامنه‌دار شدن این ضعف امنیتی دارد. البته تاکنون هیچ‌کدام از مسئولان این دو شرکت توضیحاتی در این باره ارائه نکرده‌اند و این اکسپلویت را تأیید یا رد نمی‌کنند. در این پروسه، هنوز مشخص نیست کاربران چگونه آلوده می‌شوند یا از چه نوع بدافزاری استفاده می‌شود، ولی براساس گزارش مؤسسه Fox-ITکامپیوترهای آلوده بسیار هستند و تلاش‌های ناموفق برای آلوده‌سازی توسط این کیت روی کامپیوترهای کاربران مشاهده می‌شود. این محققان هنوز موفق به شناسایی ویژگی‌های بدافزار مورد استفاده نشده‌اند و نمی‌دانند چگونه این بدافزار در کمپین تبلیغاتی گوگل توزیع می‌شود.

Malvertising به مشکل بزرگی در سال‌های اخیر تبدیل شده که در حال رشد بی‌سابقه نیز است. با وجود این‌که شبکه‌های تبلیغاتی بزرگ ادعا می‌کنند از پیچیده‌ترین سیستم‌ها و مکانیسم‌ها برای دفاع و مراقبت از تبلیغات بهره می‌گیرند، اما هنوز هکرها می‌توانند این مکانیسم‌ها را دور بزنند و کاربران را آلوده کنند. این حملات از این جهت بسیار خطرناک هستند که کاربران به‌طور خودکار و عمدی به‌سراغ بازدید از سایت‌های آلوده تبلیغاتی نمی‌روند، بلکه هکرها با قرار دادن و مدیریت یک بدافزار در شبکه‌های بزرگ تبلیغاتی، سعی در آلوده کردن کامپیوترهای قربانی از طریق نمایش یک تبلیغ در سایت‌های معتبر و تأیید شده می‌کنند.



تحقیقی که در سال 2014 روی Malvertising صورت گرفته است، نشان می‌دهد: «صنعت تبلیغات آنلاین به‌حدی رشد کرده و پیچیده شده است که هریک از طرفین (سایت نمایش‌دهنده و شرکت تبلیغ‌دهنده) می‌توانند ادعا کنند این تبلیغ آلوده از سوی آن‌ها نیست.» یکی از دلایل این وضعیت این است که یک تبلیغ آنلاین معمولی از طریق پنج یا شش واسطه قبل از نمایش روی مرورگر وب کاربر دست به دست می‌شود. در هر مرحله از این پروسه می‌توان یک بدافزار مخرب به آن افزود و همین طور این تبلیغ آلوده زنجیره‌وار ادامه یابد. از سوی دیگر، صاحبان سایت‌ها نیز هیچ کنترلی روی تبلیغات به‌نمایش گذاشته شده در وب‌سایت ندارند.

اگر مدیران وب‌سایت‌ها برای اسکن و محافظت از تبلیغات آنلاین روی سایت خود از مکانیسم‌هایی استفاده کنند یا گوگل ابزارهایی در اختیار این سایت‌ها قرار دهد که هر تبلیغ آنلاینی قبل از نمایش به‌طور کامل بررسی و از بدافزار یا اکسپلویت پاک‌سازی شود، وضعیت تبلیغات آنلاین آلوده بهبود و درصد حملات مبتنی بر این نوع آسیب‌پذیری‌ها کاهش می‌یابد. تبلیغات مانند جریان پول‌سازی هستند، گاهی مورد سوءاستفاده قرار می‌گیرند و کاربران قربانی سودجویان می‌شوند.

تاریخ انتشار:

30 اردیبهشت 1394

نشانی منبع: https://www.shabakeh-mag.com/security/657