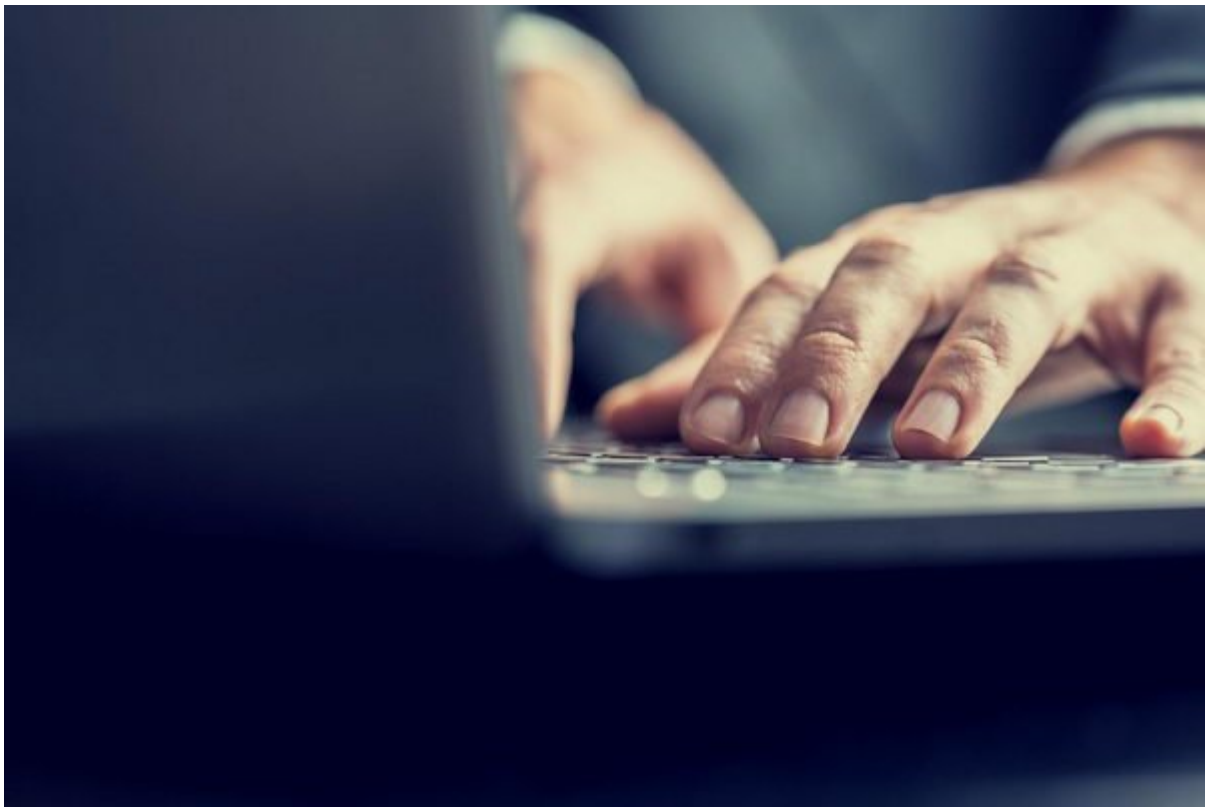
پشت پرده وب‌گردی کاربران اینترنت

چگونه تبلیغ‌کنندگان آنلاین در مورد شما می‌دانند؟

وقتی چیزی را به صورت آنلاین جستجو می‌کنید، مثلا سفر به شیراز؛ غیر عادی‌ای نیست اگر تا چند روز پس از آن به هر سایتی که سر می‌زنید تبلیغ پروازهای ارزان و تخفیف هتل می‌بینید. تعداد کمی از ما متوجه این هستیم که در پشت صحنه این تبلیغات، تا زمانی که در اختیار ما قرار می‌گیرند چه می‌گذرد. در این مقاله به این موضوع و همچنین نگرانی‌های موجود در مورد حریم شخصی می‌پردازیم.

آروین نارایانان، استادیار علوم کامپیوتر در دانشگاه پرینستون برای‌مان تشریح می‌کند: "وب مدرن یک آمیزه‌ی درهم و برهم است و بدین معناست که محتوایی که شما روی یک صفحه می‌بینید و درست مثل یک تک صفحه وب با متن و تصویر به نظر می‌رسد، در حقیقت از چندین منبع متفاوت سرهم شده است، در بعضی مواقع یک دو جین منبع، و این منابع متفاوت می‌توانند از تعدادی شرکت‌های متفاوت باشند. وقتی شما صفحه وبی را مشاهده می‌کنید، یک سری محتوا در دیدرس شما است و البته چیزهای مخفی دیگری هم وجود دارند که شما نمی‌بینید و هدف‌شان صرفا رهگیری کارهایی است که انجام می‌دهید."

تبلیغات آنلاین از روزهای ابتدایی پیدایش اینترنت با آن همراه بوده است، اما در سال‌های اخیر بسیار پیچیده‌تر شده است. تبلیغاتی که اکنون ما می‌بینیم محصول تعقیب مخفیانه دیجیتال شرکت‌هایی است که سعی در رهگیری تمام اینترنت گردی ما دارند. اما اصلا چگونه این اتفاق می‌افتد؟



چشمانی در تاریکی

نارایانان می‌گوید: "چیزی که این فناوری در آن بسیار مهارت دارد دنبال کردن شما از این سایت به آن سایت و رهگیری اعمال شما و گردآوری آن‌ها در یک پایگاه داده است که معمولا با نام واقعی نبوده، بلکه با شناسه‌های عددی استعاری صورت می‌گیرد." وی می‌افزاید: "با این وجود، او می‌داند که شما چه زمانی باز می‌گردید و می‌داند که دنبال‌تان بگردد و بر اساس پروفایلی که از قبل در مورد شما دارد، بر همان اساس با شما برخورد کرده و تصمیم می‌گیرد چه تبلیغاتی نشان‌تان دهد و چگونه محتوا را برای شما شخصی‌سازی کند و به همین ترتیب ادامه پیدا می‌کند."

ما می‌دانیم که شرکت‌ها در مورد ما اطلاعات جمع‌آوری می‌کنند، اما شفافیت بسیار کمی در چگونگی تکنیک‌هایی که آن‌ها استفاده می‌کنند وجود دارد و سوءاستفاده‌های بسیاری از این اطلاعات می‌شود. ما دقیقا نمی‌دانیم آن‌ها چه اطلاعاتی را جمع‌آوری کرده و ممکن است برای چه کاری از آن‌ها استفاده کنند.

نارایانان توضیح می‌دهد: "اطلاعاتی که بیشترین سود را برای آن‌ها دارد تاریخچه اینترنت‌گردی شما و پیشینه جستجوهای شما است. این اطلاعات در دسته‌بندی‌های رفتاری گردآوری می‌شوند." آشکار است که این داده‌ها گردآوری و آنالیز شده‌اند و برای هدف قرار دادن ما با تبلیغات مرتبط مورد استفاده قرار می‌گیرند، اما از این اطلاعات می‌توان در مسیرهای دیگری نیز بهره برد.

نارایانان می‌گوید: "این فقط رهگیری نیست بلکه استفاده از آن داده برای داده‌کاوی است و این‌که ببینید چه چیزهایی را می‌توان در مورد رفتار و ترجیحات آن فرد استنباط کرد. در برخی موارد تحقیقات نشان داده‌اند که اطلاعات حتی می‌توانند در قیمت‌گذاری مورد استفاده قرار گیرند. گاهی دیده می‌شود که یک محصول یکسان به طور زیرکانه‌ای با قیمت‌های متفاوت عرضه می‌شود."

در سال 2012، کاشف به عمل آمد که وب‌سایت مسافرتی Orbitz به کاربران مک هتل‌های گران‌تری را نسبت به کاربران PC نشان می‌دهد. بعدا در همان سال، وال استریت ژورنال گزارش کرد که وب‌سایت Staples موقعیت بینندگان‌اش را رهگیری کرده است و فقط به مشتریانی رقم تخفیف نمایش داده که یک فروشگاه رقیب در 30 کیلومتری آن فرد وجود داشته است.

آن‌ها چگونه ما را رهگیری می‌کنند؟

نارایانان می‌گوید: "مشخص شده که هر دستگاه در هنگام تعامل با کد صفحه وب بطور نامحصوصی متفاوت رفتار می‌کند، به شکلی که کاملا برای کاربر غیرقابل تشخیص است و این مسئله می‌تواند برای استنتاج یک اثرانگشت از دستگاه مورد استفاده قرار گیرد، بنابراین اشخاص ثالث می‌توانند بفهمند که همان کاربر از همان دستگاه دوباره وارد سایت شده است."

این تکنیک با عنوان انگشت‌نگاری از بوم شناخته می‌شود. وقتی یکی از این اسکریپت‌ها روی وب‌سایتی که درون آن هستید درحال اجراست، به مرورگر شما دستور می‌دهد تا یک تصویر نامرئی رسم کند. از آنجا که هر دستگاه این کار را به شیوه منحصر به فردی انجام می‌دهد، اسکریپت می‌تواند یک عدد را به دستگاه شما اختصاص داده و اینترنت گردی شما را رصد کند.

اگر این مسئله مثل چیزهای مشکوکی به نظر می‌رسد که فقط در گوشه‌های تاریک اینترنت پیدا می‌شود، پس ناامید خواهید شد وقتی بشنوید که خیلی از سایت‌های محبوب و حتی معتبر هم میزبان اینگونه اسکریپت‌ها هستند. دانشگاه Leuven بلژیک یک فهرست کامل از سایت‌هایی با این مکانیزم رهگیری را در خود دارد.

ورای ظرف شیرینی

تکنیک‌های دیگری هم برای گردآوری داده مورد استفاده قرار می‌گیرند که درک‌شان مشکل است. اکثر ما از وجود کوکی‌ها آگاهیم اما تبلیغ‌کنندگان شیوه‌های نوینی را ایجاد کرده‌اند تا سیستم کوکی را استثمار یا احاطه کند. نارایانان می‌گوید: "یکی از حوزه‌هایی که بیش از همه باعث نگرانی است، اشتراک گذاری داده‌ای است که در پشت صحنه در جریان است."

پروسه‌ای به نام همگام‌سازی کوکی به موجوداتی که درحال رصد آنلاین شما هستند امکان می‌دهد تا اطلاعاتی که از شما به دست آورده‌اند را به اشتراک بگذارند و شناسه‌هایی که برای تعیین هویت دستگاه شما ساخته‌اند را به هم مرتبط کنند. آن‌ها می‌توانند این اطلاعات را مقایسه کرده و حساب کاربری بهتری از شما بسازند. تمام این‌ها بدون آگاهی شما صورت می‌گیرد. چیز دیگری با نام سوپر کوکی وجود دارد که به طور کل سیستم کوکی معمول را نادیده می‌گیرد.

این استاد دانشگاه می‌گوید: "کوکی‌هایی در کنج مرورگر وب شما وجود دارند که امکان ذخیره‌سازی اطلاعات را فراهم می‌کنند، اما آن‌ها در پایگاه داده اصلی کوکی‌ها نیستند. یک نوع مشخص از سوپر کوکی‌ها آن‌هایی هستند که خودشان را در چندین موقعیت ذخیره کرده و از هر موقعیت برای تکثیر مجدد کوکی‌های پاک شده استفاده می‌کنند، بنابراین تا زمانی که تمام رد پاها و اشکال این کوکی‌ها را یکجا از مرورگرتان پاک نکنید، دوباره سر و کله‌شان پیدا خواهد شد."

حتی راه‌هایی وجود دارد که دو دستگاه متفاوت متعلق به یک کاربر واحد را به هم پیوند داد.

نارایانان می‌گوید: "فرض کنیم شما صاحب یک لپتاپ و یک تلفن هوشمند هستید و در سفر آن‌ها را با خود همراه دارید و از طریق وای‌فای مشغول اینترنت‌گردی هستید. تبلیغ‌کننده یا شرکتی دیگر، متوجه می‌شود که دو دستگاه

مشخص وجود دارد که همیشه از شبکه‌ای مشابه به وب‌سایت متصل می‌شود. احتمال تقارن چنین اتفاقی مشابه این است که دو نفر در یک مسیر درحال سفر باشند، بنابراین بعد از یک دوره زمانی اگر این اتفاق مدام تکرار شود آن‌ها به این نتیجه می‌رسند که همان فرد صاحب دو دستگاه متفاوت است. حالا آن‌ها می‌توانند رفتار اینترنت‌گردی شما روی یک دستگاه را در کنار رفتار اینترنت‌گردی شما روی دستگاه دیگر قرار دهند و از آن برای ساخت یک حساب کاربری عمیق‌تر استفاده کنند."

آیا ما واقعا ناشناس هستیم؟

اغلب به خورد ما داده می‌شود که شرکت‌ها تنها داده‌های بی‌نام و نشان را گردآوری می‌کنند. این همان چیزی است که نارایانان به چند دلیل به آن اعتراض دارد. وی توضیح می‌دهد که: "تاثیر شخصی‌سازی، از لحاظ قیمت‌ها و محصولات متفاوت، چه نام واقعی شما را بدانند و چه ندانند به یک میزان است. این هیچ ربطی به محاسبات و مقاصد آن‌ها در استفاده از داده‌ها برای هدف‌گیری ندارد.

نارایانان توضیح می‌دهد: "این امکان وجود دارد که با راه‌های مختلف این پایگاه‌های داده de-anonymize شوند. ما قبلا هم شاهد درز اطلاعات شخصی افراد بوده‌ایم. چیزی که فرد باید در نظر داشته باشد این است که اگر این پرونده ناشناس را در دست دارید، فقط یک کارمند بد ذات لازم است تا یک وقت، یک‌جا، هویت‌های واقعی را با آن‌هایی که در پایگاه داده ذخیره شده‌اند، مرتبط کند."

نارایانان حتی با کلمه "ناشناس" هم مخالفت دارد. دانشمندان علوم کامپیوتر از عبارت "دارای نام مستعار" استفاده می‌کنند که نه تنها بر ناشناس بودن واقعی شما تاکید دارد، بلکه یک نام مستعار هم به شما اختصاص داده شده است. اگر هویت شما فاش شود شما حریم شخصی مورد تصور خود را از دست می‌دهید و راه‌های بسیاری وجود دارد تا این اتفاق بی‌افتد.

نارایانان می‌گوید: "بسیاری از این پایگاه‌های داده‌ای که اطلاعات ما در آن گردآوری می‌شود با مقاصد بی‌غرض یا مقاصدی که مشتری با آن راحت است شروع به فعالیت کرده‌اند. اما وقتی آن را با فقدان یا ناکافی بودن شفافیت در مسئولیت و نظارت ادغام می‌کنید، یک فرصت بزرگ برای سواستفاده به وجود آورده‌اید. وقتی شرکت ورشکست شود یا پایگاه داده هک شود یا پای یک کارمند بد ذات به میان آید، چه اتفاقی می‌افتد؟"

همچنین شواهدی از رشد یک صنعت وجود دارد که هدف آن ارتباط دادن رهگیری آنلاین شما با عادات خرید آفلاین شما است. شرکت‌هایی مثل LiveRamp، راه‌هایی را ارائه می‌کنند تا این داده‌ها را به هم مرتبط کرده و دید

وسیع‌تری به شرکت‌ها دهند. اگر فروشگاهی در هنگام خرید آدرس ایمیل‌تان را از شما می‌پرسد، ممکن است آن را با شرکتی مثل LiveRamp به اشتراک بگذارد و وقتی شما وارد وب‌سایت یکی از شرکای آن‌ها می‌شوید از ایمیلی که هنگام ورود به وب‌سایت وارد می‌کنید برای تشخیص هویت شما استفاده گردد و سپس آن را با دستگاه شما مرتبط کنند. حالا آن شرکت می‌تواند نام وقعی شما را به آن داده‌ها مرتبط کند.

چگونه از حریم شخصی خود حفاظت کنیم؟

نارایانان می‌گوید: "یک راهکار جادویی برای این کار وجود ندارد. اگر کسی راهکار یا دستگاهی را به شما می‌فروشد و ادعا می‌کند که از پس تمام مشکلات در زمینه حریم شخصی برمی‌آید، مطمئن باشید که دارید نوشداروی تقلبی می‌خرید. اما اگر مصمم هستید که کمی وقت بگذارید، ممکن است بتوانید از حریم خصوصی خود محافظت کنید."

چندین افزونه مرورگر و ابزار رمزگزاری وجود دارد. نارایانان پیشنهاد می‌کند که با Ghostery شروع کنید. او همچنین توصیه می‌کند تا برای یادگیری بیشتر، وب‌سایت بنیاد مرز الکترونیک و مرکز اطلاعات حریم شخصی الکترونیک را مطالعه کنید.

نارایانان پیشنهاد می‌کند: "کمی بیشتر در مورد فناوری تحقیق کنید، در مورد فحوای حریم خصوصی محصولاتی که استفاده می‌کنید آموزش ببینید، در مورد ابزارهای حریم شخصی موجود چیز یاد بگیرید و همچنین نحوه صحیح استفاده از آن‌ها را بیاموزید. اگر شما کاملا آگاه نباشید انتخاب کاملا آگاهانه‌ای تخواهید داشت."

منبع:
دیجیتال ترندز
تاریخ انتشار:
08 تیر 1394

نشانی منبع: https://www.shabakeh-mag.com/are-network/949