

راه‌اندازی «پارسی‌جو» به تأخیر خورد!

درحالی‌که قرار بود موتور جست‌وجوی بومی «پارسی‌جو» تیرماه امسال راه‌اندازی شود، مدیران این طرح، راه‌اندازی آن را به اوایل مهرماه موکول کردند. در یازدهمین نشست شورای راهبری جویشگر (موتور جست‌جوی بومی)، اوایل مهرماه به عنوان زمان راه‌اندازی رسمی موتور جست‌وجوی «پارسی‌جو» اعلام شد. در این نشست، مدیران جویشگر «پارسی‌جو» گزارش پیشرفت طرح و آخرین وضعیت این جویشگر بومی را ارائه کردند که براساس آن در سه‌ماه آینده، فعالیت‌های در دست اجرا شامل ارتقای موتور و رساندن به کیفیت بالای ۸۰درصد گوگل (با ۱۰درصد افزایش درمقایسه‌با زمان فعلی)، راه‌اندازی سررویس‌های بومی و محلی کسب و کار، دانلود و خرید، راه‌اندازی واسط کاربر جدید و راه‌اندازی ایمیل و پروفایل سازی انجام خواهد شد.

به گفته مدیران «پارسی‌جو»، شمار کاربران این موتور جست‌وجو برای سال نخست ۵۰۰هزار، سال دوم ۲/۱ میلیون، سال سوم ۵/۲ میلیون و سال چهارم ۴میلیون کاربر پیش‌بینی شده است. همچنین شمار پرس‌و‌جوه‌ای روزانه در این جویشگر هم اکنون ۲۰۰هزار مورد است که ۳۲درصد از طریق اینترنت و ۶۸درصد از طریق اینترنت برآورد می‌شود.

«پارسی‌جو» در حال حاضر توان پاسخ‌گویی روزانه به یک میلیون پرس‌و‌جو را داراست، ضمن آن‌که شمار بازدید روزانه آن ۶۰۰هزار بازدید است که شمار کاربران یکتا ۵۵هزار کاربر و تعداد کلیک آن ۳۰۰هزار کلیک عنوان شده است. مدیران جویشگر «پارسی‌جو» همچنین مسائل کیفی شامل پیچیدگی زبان، پیچیدگی گراف وب و دشواری مسئله رتبه‌بندی، رقبای قدرتمند جهانی و بیش ذهنیت کاربران، ارائه سررویس‌های ارزش افزوده محلی و بومی مناسب، زیرساخت سخت‌افزاری و پهنای باند مناسب را چالش‌های کار خود نام بردند و با اشاره به نیروی انسانی متخصص به‌عنوان مهم‌ترین سرمایه جویشگر «پارسی‌جو»، جذب حمایت مالی برای نگهداری و جذب نیروی انسانی متخصص

را از دغدغه‌های اصلی این جویشگر عنوان کردند. سرویس‌های کنونی «پارسی‌جو» شامل جست‌وجوی وب (در ۰۰۰میلیون سندوب)، جست‌وجوی تصویر (در ۸۰۰میلیون عکس)، جست‌وجوی ویدئو (در ۵۰۰هزار فیلم)، سرویس خبرهوشمند (دسته‌بندی و طبقه‌بندی خبرها)، جست‌وجوی آوا (در یک میلیون فایل صوتی)، سرویس نقشه، سرویس روی گوشی‌های هوشمند و موبایل، سرویس تبلیغات هدمندو سرویس‌های داغ (آب و هوا، قیمت سکه، ارز و خودرو، برنامه‌های تلویزیون، بورس) است. از نگاه مدیران پارسی‌جو، راز نگهداری کاربر به عنوان مهم‌ترین مسئله موتورهای جست‌وجو در کیفیت بالای موتور و سرویس‌های کلیدی نهفته است. چرا که هزینه به‌دست آوردن مشتری جدید تا ۳۰ برابر هزینه حفظ مشتری کنونی است در حالی که هزینه بازگرداندن مشتری از دست داده ۵۰ تا ۱۰۰ برابر هزینه حفظ مشتری کنونی برآورد می‌شود. در این نشست گزارشی از دستاوردهای مهم کارگاه‌های ۹گانه طرح جویشگر بومی نیز برای اعضا شورای راهبری بیان شد و اعضا با تمدید مهلت «فراخوان مشارکت در تولید و ارائه محصول‌ها و خدمات طرح جویشگر بومی» موافقت کردند.

پیش از این دبیر شورای راهبری موتور جست‌وجوی بومی وزارت ارتباطات و فناوری اطلاعات از رونمایی رسمی از دومین موتور جست‌وجوی بومی با نام «پارسی‌جو» که ارتقا یافته نسخه آزمایشی این پروژه است، در تیرماه امسال خبر داده بود.

گوگل نتایج جست‌وجو را دستکاری می‌کند

شبیه‌سازی کرده و نتایج حاصل را با نتایجی که گوگل نمایش می‌دهد مقایسه کنند. این امر به‌خصوص درمورد جست‌وجوهای محلی کالاهای مختلف به نتایج کاملاً متفاوتی منجر شده است. تحلیل نتایج ۲۶۹۰ جست‌وجو نشان داده

که عملکرد جست‌وجوگر گوگل در ۴۵درصد موارد موجب انحراف کاربران به سمت کلیک کردن روی نتایجی شده که به‌نوعی به گوگل وابستگی داشته‌اند. گوگل مدعی است این کار را با هدف بهبود کارایی جست‌وجوگر خود انجام می‌دهد. گوگل قبلاً به‌علت این رفتار انحصارطلبانه خود با واکنش‌ها و انتقادهای تندى مواجه‌شده بودو هم‌اکنون از سوى اتحادیه اروپا به جرم انحصارطلبی تجاری تحت تعقیب است.



بررسی‌های محققان دانشگاه بیل آمریکا ثابت کرده که گوگل با دستکاری الگوریتم‌های جست‌وجوگر خود کاری می‌کند که نتایج مربوط به خدمات و سرویس‌های وابسته به این شرکت در میان برترین لینک‌ها ظاهر شود.

نتایج این بررسی که توسط گروهی به سرپرستی «تیم وو» استاد حقوق برجسته دانشگاه و مؤسسه یلپ صورت گرفته، ثابت می‌کند که به‌عنوان مثال در زمان نمایش لینک‌های مربوط به ستوران‌های برتر مورد جست‌وجوی کاربران نظرات کاربران در این مورد که در سایت‌های مختلف ثبت می‌شوند، به اندازه کافی مورد توجه قرار نمی‌گیرند. محققان برای انجام این بررسی افزونه خاصی را طراحی و به مرورگرهای اینترنتی اضافه کرده‌اند تا عملکرد موتور جست‌وجوی گوگل را

نسل جدید اینترنت بر مبنای فناوری لیزر و ماهواره

جهان نیز مورد استفاده قرار داد. در قالب این سیستم پرتوی لیزری از زمین به سوی پهپادها و ماهواره‌ها تابانده شده و انعکاس پرتوی یاد شده روی دورافتاده‌ترین نقاط کره زمین امکان‌پذیر می‌شود. تلاش برای استفاده از سیستم یاد شده به



به گفته زاکربرگ به وسیله سیستم ارتباطی لیزری جدید مشکل خدمات کندی دسترسی به وب‌سایت‌ها برطرف خواهد شد. نسل جدید اینترنت بر مبنای فناوری لیزر و ماهواره شکل می‌گیرد. یکی از شرکت‌های بزرگ فناوری از

سیستم ارتباطی لیزری جدیدی رونمایی کرده که با استفاده از آن می‌توان سرعت اینترنت را به میزان چشمگیری ارتقا بخشید. مارک زاکر برگ مدیرعامل ایس‌پوک می‌گوید این فناوری مشکل کندی دسترسی به وب‌سایت‌ها و خدمات مختلف سایبری را در برخی نقاط جهان برطرف خواهد کرد. این فناوری لیزری تبادل داده با استفاده از پهپادها و ماهواره‌ها را ممکن می‌کند و لذا می‌توان اینترنت را در نقاط دورافتاده

آغاز جنگ جهانی سوم از نوع سایبری

آنچه دوکو ۲ و ماهیت حملات آن، به ما می‌گوید



دوکو نشان داده‌اند که به معاهدات و عرف مربوط به صلح به هیچ‌وجه پایبند نیستند.

هدف قرار دادن سیستم‌های آمریکایی نیز به همین اندازه حائز اهمیت است. ایالات متحده یکی از بزرگ‌ترین قدرت‌های جهانی است که هم سرمایه نظامی خوبی دارد و هم پایتخت تکنولوژی جهان محسوب می‌شود. اینگونه جا افتاده است که ایالات متحده کشوری است که حملات سایبری را صورت می‌دهد نه آنکه هدف حملات سایبری باشد. می‌توان گفت که دوکو طراح‌ای ایالات متحده نیست. زیرا هم سیستم‌های داخلی ایالات متحده به این بدافزار آلوده هستند و هم سیستم‌هایی را آلوده کرده که هم‌زمان گروه Equation در NSA آن‌ها را هدف قرار داده‌اند. در نتیجه این فرضیه که دوکو ۲ ساخته و پرداخته اسرائیل است، قوت می‌گیرد.

همه این‌ها حاکی از آن است که به‌تدریج یک جنگ تمام‌عیار سایبری در سطح جهانی درحال وقوع است. جنگی که مرزهای قدیمی را درنوردیده و ژئوپولیتیک را حذف کرده است. توازن قوا در این‌جنگ کاملاً متفاوت است. مرزهای فیزیکی و ژئوپولیتیک اهمیت ندارند. قدرت نظامی و برتری در آن بلاموضوع است و ژنرال‌های صحنه نبرد، هکرهای توانا هستند و اتحادها و ائتلاف‌ها به واسطه ذات نامشخص این حملات، پیچیده و نامشخص. آنچه باقی می‌ماند این است که طی سال‌های آینده قطعا این جنگ با توجه به پیشرفت‌های تکنولوژیک و سرعت آن وسعت خواهد گرفت.

دوکو به ویژه دوکو ۲ مخصوصاً برای تجسس و جاسوسی از مذاکرات هسته‌ای ایران و ۵+۱ طراحی شده است. دوکو ۲ از یک لحاظ جالب توجه است و آن حملات نامقارنی است که در سطح بین‌المللی صورت داده: از تجهیزات و نهادهای ایران گرفته تا سیستم‌های دولتی در کشورهای غربی، آمریکا و جالبتر از همه خود تجهیزات کسپرسکی، به این وسیله جاسوسی مطمئن و گسترده‌ای از مذاکرات چند جانبه هسته‌ای صورت خواهد گرفت. قطعاً با هک کردن سیستم‌های ایالات متحده و کشورهای بزرگ غربی و همچنین یکی از بزرگ‌ترین و قدرتمندترین شرکت‌های امنیتی سایبری در دنیا، دوکو ۲ مرزهایی را رد کرده است که می‌تواند منجر به یک جنگ تمام‌عیار سایبری شود. انتخاب کسپرسکی به عنوان یکی از اهداف، یک موضوع را در خصوص طراحان دوکو ۲ فاش می‌کند. اول آنکه آن‌ها احمق‌هایی بی‌پروا هستند زیرا همان‌گونه که مدیرعامل کسپرسکی در صبح روز افشای حمله دوکو گفت، شرکت‌هایی مانند کسپرسکی روس و سیمانتک آمریکایی نقش صلیب سرخ را در صحنه نبرد ایفا می‌کنند. هر چقدر طرف‌های درگیر جنگ خواهان ضربه بیشتر به طرف مقابل باشند، اما همه از نقشی که این شرکت‌ها به‌عنوان امن سازندگان فضای اینترنت بازی می‌کنند، سود می‌برند. در طول تاریخ جنگ سایبری یک عرف بین همه‌هکرها از کلاه سفید تا کلاه قرمز وجود داشته است که از هدف قرار دادن مستقیم این شرکت‌های امنیتی پرهیز کنند. موضوعی که طراحان دوکو آن را برای اولین بار نقض کردند. طراحان

محققان و دانشمندان بدافزارهایی همچون استاکس نت و دوکو، زمین تا آسمان با بدافزارهایی که Xbox را هدف قرار دادند، متفاوت هستند. این بدافزارهای نخبه‌زمانی که شروع به فعالیت کنند، به شکل هوشمندانه‌ای اجازه ورود هدایت‌کنندگان به شبکه‌های پیچیده، حتی پیچیده‌ترین و امن‌ترین آن‌ها را می‌دهند و قادر به استخراج داده‌های ذخیره شده، ثبت و ضبط کلیدها و گذروژه‌ها و حتی کنترل صنایع سنگین و زیرساختی همچون تجهیزات هسته‌ای، نیروگاه‌ها و برج‌های مراقبت هوایی هستند. درواقع بدافزارهایی نظیر استاکس نت قادر به ایجاد همان چیزی هستند که می‌توان از آن به استعاره به‌عنوان قیامت یاد کرد. در حالی که دوکو ۲ تا حد زیادی بر اساس کد استاکس نت طراحی شده است، اما مأموریت آن متفاوت است. استاکس نت به‌عنوان بدافزاری ساخته شده با همکاری ایالات متحده و اسرائیل برای جاسوسی از برنامه هسته‌ای ایران و ایجاد اختلال در روند غنی‌سازی اورانیوم ایران شناخته شده. مأموریتی که در نهایت با شکست مواجه شد. اما رهیافت جدیدی که استاکس نت برای کنترل از راه دور تجهیزات و صنایع به‌دست داد، فصل جدیدی در کتاب آینده جنگ سایبری بود.

اما در سوی دیگر خانواده دوکو و حملات آن بیش از آنکه روی کنترل تمرکز داشته باشد، روی جاسوسی متمرکز است و در واقع بخشی از عملیات استاکس نت را تقویت کرده و استفاده می‌کند. البته هنوز این خانواده هدف اصلی خود را ایران می‌داند اما نه به‌وسیله عملیات تخریبی بلکه خانواده

اکنون برای چندی سال متمادی است که مؤسسات امنیت سایبری هشدارهای پیاپی مبنی بر احتمال وقوع جنگ جهانی سوم اما از نوع سایبری می‌دهند. این موضوع در جایی معنا می‌یابد که هکرها با ابزار‌های پیشرفته خود توان نفوذ به تأسیسات حساس ابرقدرتی همچون ایالات متحده را دارا هستند و می‌توانند واقعه «پرل هاربور» را بار دیگر رقم بزنند. اکنون بنا به دلایلی خاص دیده می‌شود که اغلب بدافزارهای جاسوسی پیشرفته سیستم‌های آمریکایی را آلوده کرده یا هدف قرار داده‌اند. در حالی که هیچ‌کس چندان به اهمیت این موضوع توجه نمی‌کند.

در واقع سخن از یک بدافزار ویژه و خاص است. بدافزاری که از سوی شرکت امنیت سایبری کسپرسکی در ماه ژوئن کشف شد و اذعان شد که از حدود یک سال گذشته روی اغلب سیستم‌های حساس آمریکا و به طریق مشابه در سراسر دنیا شیوع یافته است و شباهت بسیاری به «استاکس نت» دارد. این بدافزار جدید نسخه تحول‌یافته خلف خود Duqu است که با نام ۲ Duqu خطاب می‌شود.

آنچه بیش از همه کارشناسان امنیت سایبری را از بابت این بدافزار نگران می‌کند، سطح بالای پیچیدگی عملکرد آن و همچنین بی‌پروایی در حمله به اهداف است. برای بدافزارهایی پیشرفته مشغول طراحی و تولید بدافزارهایی بوده‌اند که به‌وسیله آن‌ها قادر به جاسوسی تمام‌عیار از برخی اهداف مشخص باشند. اهدافی نظیر مذاکرات هسته‌ای ایران، رهبران ایرانی و سایر رهبران جهانی، شرکت‌های مخابراتی و ارتباطی و همچنین

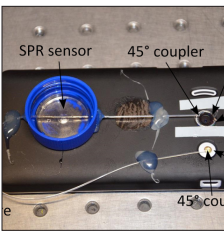
آیا این گوشی اندرویدی بلک‌بری است؟



به‌تازگی Evan Blass شخصی که با اکانت توییتر خود به نام @evleaks شهرت یافته، یک رندر کامپیوتری با کیفیت از موبایل جدید بلک‌بری، مجهز به پلتفرم اندروید را

در حساب کاربری توییتر خود منتشر کرده و اظهار نموده که این موبایل با نام «وینز» به بازار عرضه می‌گردد. این تصویر بیانگر این موضوع است که شایعات پیشین نیز صحت داشته و موبایل وینز با نامیشرگی از هر دو سو

گوشی‌های هوشمند با رداری را تشخیص می‌دهند



حققان «مرکز فناوری‌های اپتیکی هانوفر» (HOT) وابسته به دانشگاه هانوفر آلمان حسگرهایی حاوی فیبرنوری برای گوشی‌های هوشمند ساختند که می‌تواند انواع مختلف آزمایش‌های

بیومولکولی را انجام دهد که از جمله این آزمایش‌ها می‌توان به تشخیص بارداری یا ماینورینگ دیابت اشاره کرد. اطلاعات به دست آمده از این حسگر توسط یک ابزار کاربردی که روی گوشی هوشمند نصب شده است خوانده می‌شود و

نسل دوم گوگل گلس با نام GG1

زبادی نیز در خصوص ظاهر گوگل‌گلس در آن عنوان نشده است. از سوی دیگر می‌توان گفت که بیشتر اطلاعات مربوط به بخش نرم‌افزاری محصول هستند. هرچند صرفاً عنوان شده که



گلس، روی یک عینک مستطیل شکل قرار خواهد گرفت و از طریق یک بخش کناری نیز می‌توان به منوهای آن دسترسی پیدا کرد. این بخش کناری احتمالاً همانند تاج پد نسل قبل خواهد بود که در کنار عینک قرار داشت.

بر اساس اسناد منتشر شده از کمیسون ارتباطات فدرال آمریکا، مشخص گشته که گوگل به‌شکل فعال در حال انجام آزمایش‌هایی درخصوص نسخه دوم گوگل گلس

است. به‌طور کلی، در اسناد یاد شده مشخص شده که نسخه جدید محصول مورد بحث از جدیدترین تکنولوژی‌های مربوط به Wi-Fi و بلوتوث بهره‌می‌گیرد. در میان این اسناد، از نسخه جدید با نام GG۱ یاد شده و جزئیات