اهداف فاوای نفت

دستیابی به صنعت نفتی مبتنی بر اندیشه و خرد با محوریت فاوا

ارتقای دانش با محوریت سرمایه فکری به منظور افزایش کارآیی و اثربخشی

ایجاد بسترهای مناسب و مطلوب فاوا جهت دستیابی به صنعت نفت پیشرفته

ارتقاء کارایی و اثر بخشی ارکان مدیریتی و اجرایی از طریق فاوا در صنعت نفت

برنامه‌ریزی و هوشمند سازی فرایندهای کسب‌وکار الکترونیک صنعت نفت

استقرار فراگیر و یکپارچه کاربردها و خدمات فاوا در صنعت نفت

خبرنامه فاوای نفت

فاوای نفت

تاریخ انتشار ۹۶/۰۶/۰۱ شماره خبرنامه ۴۰۰

در این شماره می خوانید:

خبرنامه فاوای نفت از مطالعه همدان در خصوص ارائه مطالب و پیشنهادات دعوت به مشارکت می نماید

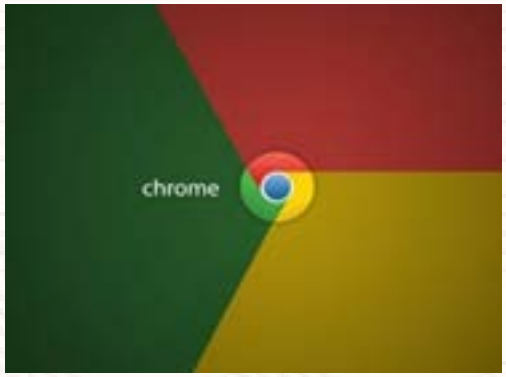
داستان حذف برنامه‌های ایرانی از اپ استور اپل چه بود؟

شرکت اپل اخیرا و بدنبال تحریم‌های سیاسی و اقتصادی ایالات متحده آمریکا علیه ایران، برنامه‌ها و اپلیکیشن‌های ایرانی را از فروشگاه اینترنتی اپ استور خود حذف کرد.نیویورک تایمز در گزارشی نوشته است با اینکه شرکت اپل در ایران بصورت رسمی دارای نمایندگی نیست اما ایرانی های بسیاری از محصولات آن نظیر گوشی‌های هوشمند آیفون، آیپد، آیپاد و سایر محصولات و سرویس های دیگر آن استفاده می‌کنند و حذف برنامه‌ها و اپلیکشن‌های ایرانی از فروشگاه اپ استور، مشکلات و محدودیت‌هایی برای آنها ایجاد خواهد کرد. این در حالیست که در هفته‌های گذشته شرکت آمریکایی اپل به مقابله جدی علیه نرم‌افزارهای غیرقانونی چینی برای دور زدن فیلترینگ و دسترسی بدون محدودیت به اینترنت پرداخته بود.بدنبال این اقدام اپل، برخی کاربران ایرانی اعتراض خود را در فضای مجازی اعلام کرده‌اند و محمدجواد آذری جهرمی، وزیر ارتباطات ایران، در صفحه توییتر خود نوشت:» احترام به حقوق مشتریان در جهان امروز، یک اصل بشمار می‌رود که اپل اکنون آن را زیر پا گذاشته است. ما بطور قانونی حذف برنامه های ایرانی از اپ استور را پیگیری خواهیم کرد».
شرکت اپل در پیامی به توسعه‌دهندگان ایرانی که تحت تاثیر این اقدام اپل قرار گرفته اند، به وضوح اعلام کرده است که طبق قوانین و ضوابط این نرم افزار، به کشورهای تحت تحریم سرویسی داده نمی شود؛ سخنگوی شرکت اپل، صحت این مطلب را تایید اما از اظهار نظر بیشتر خودداری کرده است.
از زمانی که ریاست جمهوری ایالات متحده آمریکا تغییر یافت، سیاست های ارتباطی و اینترنتی بسیاری نیز دستخوش تغییر شد. دولت باراک اوباما – رئیس جمهور پیشین آمریکا – بمنظور گسترش و سهولت ارتباطات در ایران، از تاثیرگذاری تحریم‌های سیاسی و اقتصادی بر فضای مجازی اندکی کاسته بود اما در دولت ترامپ، باری دیگر سیاست‌های تحریم گرایانه به روی کار آمده و کشورها و موسسات و افراد بسیاری را تحت الشعاع قرار داده است.بر اساس این گزارش البته بنظر می‌رسد ایرانی‌ها با توجه به استفاده گسترده‌ای که از سرویس‌های آنلاین و اینترنتی دارند، به دنبال راه‌های جدیدی باشند تا حتی با وجود تحریم‌ها، بتوانند از خدمات مورد نیازشان استفاده کنند.

راه‌اندازی فایروال برای اپ انجین توسط گوگل

به گزارش شبکه خبری **ICTPRESS**، شرکت گوگل اعلام کرده که قابلیت فایروال جدیدی راه‌اندازی و برای توسعه‌دهندگان و مدیران، این امکان را فراهم ساخته است که از اپ انجین استفاده کنند و دسترسی به منابع خاص ترافیک را به راحتی محدود نمایند.گوگل اپ انجین (جی.اِی. ای)، یک پلتفرم مدیریت‌شده در مجموعه خدمات گسترده گوگل‌کلود است که با خدمات وب آمازون (ای.دبلیو.اس) و مایکروسافت اژور رقابَت می‌کند. اپ انجین، چارچوب و پلتفرمی برای توسعه و گسترش اپلیکیشن‌هایی است که در فضای ابری گَوگل بارگذاری می‌شوند.توسعه‌دهندگان، خواه در طول آزمایش و خواه به دلایل دیگر، ممکن است بخواهند اپلیکیشن جدیدی را صرفاً برای گروه خاصی از کاربران باز کنند یا آن اپلیکیشن را از دسترسی منطقه خاصی از جهان خارج سازند. در حال حاضر این امکان وجود دارد که بر اساس آدرس آی.پی، دسترسی به اپلیکیشن مورد نظر را محدود کنند؛ البته این موضوع نیازمند کنترل دسترسی درون کد است.

اقدام کروم بر علیه سایت‌های پرسروصدا



امروزه بسیاری از وب‌سایت‌ها حاوی ویدئوهایی هستند که به طور خودکار پخش شده و سروصدای آنها ممکن است باعث آزار مخاطب شود.به نقل از تک کرانچ، طراحان مرورگر کروم با درک این مشکل، نسخه جدید این مرورگر را به گونه ای طراحی کرده‌اند که ساکت کردن کامل هر وب سایتی را ممکن می‌کند. تنظیمات اجرا شده به این شیوه به طور دائمی بر هر سایتی قابل اعمال خواهد بود.

کروم از چندسال قبل علامت زدن سایت‌های پرسروصدا و آزاردهنده و ارسال اطلاعات مربوط به آنها را برای گوگل ممکن کرده بود و حالا این قابلیت را به طور آزمایشی توسعه داده و در حال تست آن در نسخه **Canary** است.برای فعال کردن این قابلیت تنها کافیست بر روی گزینه مربوط به بخش امنیت یا **security** کلیک کنید که در گوشه سمت چپ آدرس وب سایت قرار دارد و سپس گزینه ساکت کردن وب سایت را از فهرست جزییات و مجوزها انتخاب کنید. کاربران در صورت تمایل می توانند این تنظیمات را تغییر دهند.انتظار می‌رود با ارائه خدمات مشابه در دیگر مرورگرها، طراحان وب‌سایت‌ها از گنجاندن ویدئوهای پرسروصدا که به طور خودکار پخش می شوند خودداری کنند.

سرویس‌های اینترنتی مایکروسافت؛ طعمه هکرها

مایکروسافت طی انتشار آخرین نسخه از گزارش امنیت اطلاعات خود (SIR)، چشم اندازهای سایبری، نرم‌افزارهای مخرب، سواستفاده‌های اینترنتی و حملات سایبری به حساب‌های شخصی و سازمانی را تحلیل کرده است. دانستن این گونه اطلاعیه‌ها که توسط مایکروسافت منتشر می‌شود، می‌تواند کمک بسزایی به حفاظت اطلاعات سازمان‌ها و اشخاص کند.طبق گزارش وب‌سایت techrepublic، اغلب این سواستفاده‌های اینترنتی به دلیل گذرواژه‌های ضعیف و قابل حدس کاربران و مدیریت ضعیف آن بوده است که حملات فیشینگ و نفوذ به سرویس‌های شخص ثالث را بدنبال داشته است.بر اساس یک گزارش سالانه، امنیت اطلاعات دیگری که توسط مایکروسافت منتشر شده، میزان تلاش IP های ناشناس برای ورود به اکانت های اینترنتی، در سه ماهه نخست سال ۲۰۱۷ در مقایسه با سه ماهه نخست سال ۲۰۱۶، ۴۴ درصد افزایش داشته است.این گزارش همچنین افشا کرد که بالغ بر دو سوم این IP های ناشناس از کشورهای ایالات متحده آمریکا و چین به ترتیب با نرخ ۳۲.۵ درصد و ۳۵.۱ درصد انجام گرفته و کره هم در سومین جایگاه با ۳.۱ درصد قرار گرفته است.مایکروسافت با هدف بهبود امنیت و حفاظت اطلاعات کاربرانش، روش های گوناگونی را به کار گرفته است. به عنوان مثال، این شرکت آنتی ویروس ویندوز دیفندر را در کامپیوترها و تمامی دستگاه‌هایی که دارای ویندوز ۱۰ بوده و از نرم افزار آنتی ویروس دیگری استفاده نمی‌کنند، به طور پیش فرض فعال می کند.همچنین سازمان‌های مختلف برای افزایش ضریب امنیت و حفاظت اطلاعات خود، می توانند از سرویس های مایکروسافت همانند مدیریت هویت مجاز، اهراز هویت چند عاملی آژور و هلو برای کسب و کار بهره ببرند.مایکروسافت و سایر سرویس دهندگان آنلاین هم به کاربران و سازمان‌ها توصیه می کنند که در حساب‌های خود از گذرواژه‌های قدرتمند و با کاراکترهای مختلفی استفاده کنند.

طراحی هوش مصنوعی ویژه برای تعیین کیفیت خواب

به گزارش شبکه خبری **ICTPRESS**، به‌تازگی دانشمندان یک سیستم هوش مصنوعی جدید طراحی کرده‌اند که می‌تواند با استفاده از امواج رادیویی، وضعیت و کیفیت خواب انسان‌ها را اندازه‌گیری و تحلیل کند.بررسی وضعیت خواب به کمک فناوری امر چندان جدیدی نیست ولی برای این کار همواره به دستگاه‌های جانبی نیاز بوده است.

حال دانشمندان روش جدیدی برای این کار ابداع کرده‌اند که به کمک این روش دیگر نیازی به استفاده از حسگرهای مختلف بر روی بدن کاربر نخواهد بود بلکه این مدل کاری جدید به سراغ بررسی وضعیت خواب بر پایه تحلیل بدن انسان به کمک امواج رادیویی رفته است.این روش جدید به تحلیل امواج رادیویی اطراف انسان‌ها می‌رود و مقادیر برداشت شده را بر اساس وضعیت‌های مختلف (سه وضعیت مختلف) خواب تعبیر می‌کند.

وضعیت‌های خواب در نظر گرفته شده برای این هوش مصنوعی شامل خواب سبک، خواب عمیق و خواب با تحرک مردمک چشم فرد هستند.این پروژه که توسط مرکز تحقیقات **MIT** انجام شده است، می‌تواند تحلیل وضعیت بیماران و حتی افراد عادی را نیز دستخوش تغییراتی شگفت‌انگیز کند و با توجه به تکیه آن بر استفاده از هوش مصنوعی، به‌راحتی می‌توان در آینده آن را بهبود بخشیده و برای نیازهای پیش رو آماده کنند.

هشدار مایکروسافت مبنی بر حملات روزافزون هکرها به حساب‌های ابری

شرکت مایکروسافت هشدار داده که هکرها به شکلی روزافزون، اعتبار ابری کاربران را هدف قرار می‌دهند، به‌طوری‌که تعداد حملات این هکرها در سه ماهه نخست سال ۲۰۱۷ سه برابر شده است. آخرین گزارش امنیتی مایکروسافت نیز بیانگر آن است که حساب‌های کاربران در نتیجه رمزعبورهای ضعیف و قابل حدس و همچنین مدیریت ضعیف پسوردها، در معرض خطر قرار می‌گیرد و به همین خاطر میزان حملات فیشینگ و نقض سرویس‌های شخص ثالث به شکل فزاینده‌ای رو به رشد است.در گزارش مذکور همچنین آمده است: «تعداد ورود به حساب‌های مایکروسافت از آدرس‌های آی.پی مخرب در سه ماهه نخست سال ۲۰۱۷، نسبت به سه ماهه نخست سال ۲۰۱۶، به میزان ۴۴ درصد رشد داشته است.» به نقل از اینکوایرر، همچنین در ادامه گزارش ذکر شده است: «این احتمال وجود دارد که خط مشی امنیتی مبتنی بر دسترسی مشروط، شامل مقایسه آدرس آی.پی دستگاه درخواست‌دهنده به مجموعه‌ای از آدرس‌های آی.پی یا دستگاه‌های مورد اعتماد، بتواند به کاهش خطر سوءاستفاده از اعتبار، کمک نماید.»

از سوی دیگر، حساب‌ها و اعتبارهای بیشتری به صورت آنلاین در معرض خطر هک شدن قرار می‌گیرد و هکرها را قادر می‌سازد تا از ورودی‌های مشابه نام و رمز عبور برای ورود به حساب‌ها استفاده نمایند. در این زمینه، مایکروسافت نیز سیستم‌های خودکاری را راه‌اندازی کرده است که می‌تواند این حملات را تشخیص دهد و هر روز میلیون‌ها حمله را مسدود و برطرف نماید.وقتی یک هکر از یک اعتبار معتبر استفاده می‌کند، این درخواست با چالش روبرو می‌شود و از کاربر خواسته می‌شود که برای ورود به سیستم، اعتبار بیشتری ارائه دهد. در این‌گونه مواقع، هکرها مانند کاربران واقعی رفتار می‌کنند و وظیفه حفاظت از حساب‌ها را به شکلی مستمر انجام می‌دهند.از نقطه نظر فنی، می‌توان برخی از فناوری‌ها را برای به حداقل رساندن چنین خطراتی مورد استفاده قرار داد.نکته مهم در این میان عبارت از این واقعیت است که وقتی سازمانی به سمت فضای ابری حرکت می‌کند، باید مسائل امنیتی را در اولویت اصلی کار خویش قرار دهد. مایکروسافت هشدار داده که یک هکر در یک سناریوی تهدید فضای ابری، با هجوم به یک زیرساخت ابری، کنترل یک یا چند ماشین مجازی را در دست می‌گیرد و سپس از این ماشین مجازی برای حملات دیگر خود استفاده می‌کند.