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

۴۲۷ شماره خبرنامه ۹۷/۰۲/۲۶ تاریخ انتشار

در این شماره می خوانید:

- هوش مصنوعی
- رفع فیلتر تلگرام
- Safe Links
- بیت کوین
- آی مسیج

خبرنامه فاوای نفت از عاقله صدیق در خصوص ارائه مطلب و پیشنهادات دعوت به مشارکت می نماید

تهدیدهای هوش مصنوعی و نگرانی جامعه جهانی

موضوع منتخب امسال برای اتحادیه بین‌المللی ارتباطات همزمان با روز جهانی ارتباطات، استفاده مثبت، بهینه و مفید از فناوری هوش مصنوعی اعلام شده است. دومین رویداد از اجلاس جهانی استفاده درست و مثبت از هوش مصنوعی در تاریخ ۱۵ تا ۱۷ ماه مه سال جاری ۲۰۱۸ میلادی در شهر ژنو سوئیس برگزار خواهد شد. همانطور که از نام این رویداد جهانی معلوم و مشخص است، موضوع اصلی و منتخب آن، استفاده بهینه و مثبت از فناوری هوش مصنوعی است.

از آنجا که فناوری هوش مصنوعی و یادگیری ماشینی در سال‌های اخیر با پیشرفت قابل ملاحظه‌ای مواجه شده است و غول‌های تکنولوژی متعددی همچون گوگل، مایکروسافت، آمازون، اپل، سامسونگ و غیره به طراحی و ساخت ابزارهای هوشمند مبتنی بر فناوری هوش مصنوعی (Artificial intelligence) بسیاری روی آورده‌اند. جدیدترین نمونه‌ای که سرو صدا و جنجال‌های بسیاری را در جهان به پا کرد، دستیار صوتی مبتنی بر هوش مصنوعی گوگل دوپلکس بود که صدای آن شباهت بسیار بی‌نظیری به صدای انسان دارد به گونه‌ای توسط کاربران قابل تشخیص نیست که مخاطب یک روبات است نه یک انسان!

بسیاری از منتقدان هوش مصنوعی بخصوص ابزار گوگل دوپلکس بر این باورند که توسعه و گسترش این فناوری می‌تواند خطرات و تهدیدات جبران‌ناپذیری را برای جهانیان ایجاد کند و آینده زمین را به شدت به مخاطره بیاندازد. حالا موضوع و محور اصلی اجلاس جهانی استفاده مثبت از هوش مصنوعی (AI for Good) که در راستای روز جهانی ارتباطات برگزار می‌شود، نیز بررسی احتمال سوءاستفاده و اندیشیدن استراتژی‌های کاربردی به منظور جلوگیری از مصارف نامناسب و مجرمانه از فناوری هوش مصنوعی خواهد بود. جالب است بدانید که استفن هاوکینگ، الون ماسک، استیو ووزنیاک، بیل گیتس و بسیاری دیگر از نام‌های بزرگ در زمینه علم و فناوری، مدتهاست که در رسانه‌ها و نامه‌های سرگشاده‌ی خود، درباره خطرات ناشی از هوش مصنوعی ابراز نگرانی کرده و به خیل محققان برجسته‌ی هوش مصنوعی پیوسته‌اند. خطراتی که می‌تواند به مجرمان این امکان را بدهد تا با سرعت و دقت بیشتری و با کمترین زحمت و احتمال ردیابی، به انجام سرقت، قتل‌های زنجیره‌ای، فریب افراد و کلاهبرداری‌های تلفنی و اینترنتی بپردازند.دیگر مسائل و موضوعاتی که به محور اصلی این رویداد یعنی هوش مصنوعی نزدیک است و مورد بحث و گفت‌وگو قرار می‌گیرد، می‌توان به یادگیری ماشینی، داده‌های بزرگ، توان رایانشی، ظرفیت ذخیره‌سازی حافظه و سایر فناوری‌های در حال توسعه و جدید مبتنی بر هوش مصنوعی اشاره کرد.

وزیر ارتباطات در پاسخ به ICTPRESS: شخصا با تلگرام مخالف نیستم اما رفع فیلتر نمی کنند

محمد جواد آذری جهرمی با تاکید بر اینکه تلگرام دیگر رفع فیلتر نمی شود گفت: شخصا با این پیام رسان مشکلی ندارم. وزیر ارتباطات و فناوری اطلاعات در حاشیه برگزاری آیین بهره برداری از مرکز عملیات شبکه شرکت مخابرات ایران صبح روز دوشنبه ۲۴ اردیبهشت ۹۷ در پاسخ به سوال شبکه خبری آی سی تی پرس مبنی بر اینکه آیا به عنوان وزیر ارتباطات با فیلتر تلگرام موافق هستید؛ برای رفع آن با توجه به اینکه میزان بالایی از مردم هنوز از این پیام رسان استفاده می کنند و به آن اقبال دارند چه برنامه ای دارید، تصریح کرد: برای رفع فیلتر آن چه کار می توانم انجام دهم، اما با فیلتر آن نیز موافق نیستم.محمد جواد آذری جهرمی در ادامه گفت: شخصا با پیام رسان تلگرام مشکلی ندارم و با آن مخالف نیستم.وی تاکید کرد: بعید می دانم دیگر تلگرام رفع فیلتر شود؛ فیلتر تلگرام را لغو نخواهند کرد.

وزیر ارتباطات همچنین در پاسخ به سوالی مبنی بر اعتراض یکی از پیام‌رسان‌ها درباره چالش‌های نرم‌افزاری زیرساخت و اپراتورها اظهار کرد: ما در کشور پنج پیام‌رسان داریم، این که یکی از آن‌ها به جای طرح موضوع در جلسات مرتبا بحث را به موضوع عملیات روانی بکشاند، نه به سود آن‌هاست و نه به سود کشور.جهرمی ادامه داد: وزارت ارتباطات و اپراتورها بنایشان بر همکاری تمام مدت با پیام‌رسان‌هاست و این موضوع را به عنوان یک تکلیف مهم ملی پیگیری می‌کند، بنابراین ایجاد عملیات روانی، ذهنیتی ایجاد می‌کند و تاثیر منفی دارد و اگر کسی مشکلی دارد باید با استدلال و استناد پیگیری کند.وزیر ارتباطات و فناوری اطلاعات، خاطرنشان کرد: نمی‌شود چهار پیام‌رسان دیگر خوب کار کنند و یک پیام‌رسانی که ادعایی داشته و به آن نرسیده شروع به پروپاگاندا کرده و مسئولیت را به گردن دیگران بیندازد. توصیه ما این است که پیام‌رسان‌ها بدانند ما از آن‌ها حمایت کرده و مشکلات را پیگیری و برطرف می‌کنیم.

حمله ای که ویژگی امنیتی Safe Links را در آفیس ۳۶۵ دور می‌زند!

به تازگی محققان امنیتی روشی را کشف کرده‌اند که گروه های هکری با استفاده از آن توانسته‌اند ماژول امنیتی مایکروسافت آفیس ۳۶۵ را که در اصل برای حفاظت از کاربران مقابل حملات فیشینگ و بدافزارها طراحی شده است را دور بزنند.به گزارش سرویس اخبار تکنولوژی از کسپرسکی آنلاین، این ماژول در نرم افزار ۳۶۵ آفیس به عنوان یک راهکار امنیتی پیشرفته ATP وجود دارد که تمام URLها را در ایمیل‌های دریافتی با URLهای امن مایکروسافت جایگزین می کند. بنابراین هر بار که کاربر بر روی یک لینک در ایمیل کلیک می‌کند ابتدا به یک دامنه متعلق به مایکروسافت هدایت می شود که مایکروسافت فورا URL اصلی را برای وجود هرگونه مورد مشکوکی بررسی می‌کند. در صورتی که اسکنر مایکروسافت مورد مخربی را بررسی کند به کاربران در مورد آن هشدارهای لازم را می دهد و در صورتی که موردی یافت نشود کاربر به URL اصلی هدایت می شود.
با این حال محققان شرکت امنیتی Avanan نشان داده‌اند که مهاجمان چگونه از طریق تکنیک baseStriker attack از ویژگی Safe Links در مایکروسافت عبور کرده اند.حمله BaseStriker شامل برچسب <base> در هدر یک ایمیل HTML است که برای تعیین یک URI پایگاه پیش فرض یا یک URL برای لینک‌های وابسته در یک سند یا صفحه وب مورد استفاده قرار می گیرد.به بیانی دیگر، اگر URL از نوع <base> تعریف شده باشد، تمام لینک های مرتبطِ بعد از آن، از آن URL به‌عنوان نقطه شروع استفاده می‌کنند.
همانطور که در تصویر بالا نشان داده شدهٔ است محققان امنیتی یک کد HTML مربوط به یک ایمیل فیشینگ را با یک کد که از برچسب <base> برای توزیع لینک مخرب استفاده می‌کند، به طوری که ویژگی Safe Links قادر به شناسایی و جایگزینی آن لینک نباشد را مقایسه کردند که درنهایت قربانیان را هنگام کلیک به سایت‌های فیشینگ هدایت می کند. محققان این حمله را بر روی پیکربندی تست کردند و یافتند که هر کاربری که از آفیس ۳۶۵ استفاده می کند، اسیب پذیر است. چه این پیکربندی ها کلاینت اینترنت باشند، چه برنامه تلفن همراه یا یک برنامه دسکتاپ اوت لوک!
تا به حالا محققان امنیتی مجرمانی که تنها از حمله baseStriker برای ارسال ایمیل های فیشینگ استفاده کرده اند را مشاهده کرده‌اند اما بر این باور هستند که این حمله می تواند برای توزیع باج افزارها، بدافزارها و دیگر نرم افزارهای مخرب مورد استفاده قرار گیرد.Avanan این مسئله را به کمپانی مایکروسافت و Proofpoint گزارش داده است اما تا به حال هیچ راهکاری برای آن ارائه نشده است.

رابطه بیت کوین و وام در آلمان

بانکی به نام بیت باند در آلمان تاسیس شده تا مشتریان با بیت کوین وام‌هایشان را به هرجای دنیا انتقال دهندیک شهروند آلمانی، یک بانک آنلاین تاسیس کرده که به مشتریان خود اجازه می‌دهد با استفاده از بیت‌کوین، وام‌هایشان را به هر جای دنیا منتقل کنند .به گزارش سرویس اخبار تکنولوژی از ایسنا، این بانک به نام «بیت باند» از ارزهای مجازی چون بیت کوین برای دور زدن سیستم بین‌المللی سوئیفت استفاده می‌کند تا به سرعت و با هزینه‌ای پایین در سراسر جهان فرآیند استقراض انجام شود. رادوسلاو آلبرشت در دفتر خود در برلین به رویترز گفت: انتقال سنتی پول به دلیل تعرفه‌های نرخ ارز، پرهزینه بود و می‌توانست چند روز به طول بینجامد. بیت باند مستقل از محل مشتری کار می‌کند و با استفاده از اینترنت، کار بسیار سریع و کم هزینه صورت می‌گیرد.

مشتریان باید وام‌های گرفته شده در قالب دیجیتالی نظیر بیت کوین را برای چند ثانیه یا دقیقه نگه دارند تا این ارز به ارز کشوری که مشتریان می‌خواهند وجوه خود را دریافت کنند، تبدیل شود تا بدین وسیله از ایجاد نوسان در نرخ تبدیل ارزهای مجازی نیز خودداری شود..!

استفاده از آی مسیج در ویندوز ممکن می شود

مایکروسافت اعلام کرد که در ویندوز، یک اشکال بحرانی پیدا شده است. متخصصان این حوزه اعلام کردند که این باگ امنیتی، هم‌اکنون در معرض حمله است. قرار است که مایکروسافت مطابق وعده خود، دو اشکال را پچ یا به اصطلاح «وصله» کند.از نظر کارشناسان، از میان ۶۷ باگی که در بروزرسانی ماه مه اعلام شد، این دو اشکال به صورت جدی در معرض حمله هستند. بروزرسانی سه‌شنبه پچ مایکروسافت به موتور "**VBScript**" ویندوز پرداخته است. در حال حاضر، هکرها تلاش می‌کنند از طریق ماشین‌های ویندوز و اینترنت اکسپلورر، از این اشکالات سوءاستفاده کنند.به نقل از زد.دی نت، این پچ به دنبال هشداری عرضه شد که پژوهشگران در ماه آوریل ارائه نمودند. هکرهای کارآزموده از این اشکالات سوءاستفاده کرده تا کامپیوترهای ویندوز را در مقیاس جهانی آلوده سازند. پژوهشگران مایکروسافت و تحلیلگران باج‌افزار آزمایشگاه کسپرسکی، بلافاصله تحقیقات خود برای کشف باگی بحرانی را آغاز نمودند.

مایکروسافت به هیچ‌وجه تأیید نکرده که گزارش این باگ توسط "**Qihoo ۳۶۰ Core Security**" منتشر شده است، لیکن توضیح داده که می‌توان از طریق اینترنت اکسپلورر از این باگ سوءاستفاده نمود. مایکروسافت همچنین اعلام کرد: «در سناریوی حمله مبتنی بر وب، مهاجم می‌تواند یک وب‌سایت را به عنوان میزبان بکار گیرد. این وب‌سایت برای سوءاستفاده از آسیب‌پذیری طراحی شده و سپس کاربر را فریب می‌دهد تا از وب‌سایت موردنظر، دیدن کند.»گفتنی است حملاتی که از طریق این آسیب‌پذیری انجام شده، بیشتر با استفاده از اسناد **Word** آفیس بوده است، بدین‌ترتیب کاربر با باز کردن اسناد، در معرض حمله قرار می‌گیرد. حملات روز صفر، توسط هکرهای ماهر انجام می‌شود و این نوع از حمله نیز از نوع حملات روز صفر است.حمله صفر روزه یا حمله روز صفر، حمله یا تهدیدی رایانه‌ای است که از یک آسیب‌پذیری در نرم‌افزاری کاربردی که تا پیش از این ناشناخته بوده است بهره‌جویی می‌کند. این بدان معناست که توسعه‌دهندگان برای رفع آسیب‌پذیری، صفر روز فرصت داشته‌اند. پیش از آنکه توسعه‌دهنده نرم‌افزار، از هدف آسیب‌پذیری آگاهی یابد، سوءاستفاده صفرروزه (نرم‌افزاری که از یک حفره امنیتی برای اعمال یک حمله استفاده می‌کند) توسط حمله‌کنندگان استفاده یا به اشتراک گذاشته می‌شود.

بدافزاری خطرناک در گوگل پلی

این بدافزارها جلوی پاکسازی را می‌گیرند و وب‌سایت‌های آلوده را در معرض دید کاربر قرار می‌دهند. به نقل از مهر، شرکت امنیتی سمانتک از شناسایی تعدادی بدافزار جدید و خطرناک خبر داد که تداوم حضور آنها در گوگل پلی کاربران را به طور جدی تهدید می کند. بدافزارهای یادشده قبلا هم در گوگل پلی وجود داشته و حذف شده بودند، اما حالا با اسامی جدید به این فروشگاه آنلاین بازگشته اند.این بدافزارها در برنامه های موبایلی مختلفی مخفی شده اند که برخی از آنها هم دارای محبوبیت هستند و همین مساله می تواند تعداد افرادی که به علت نصب برنامه های مذکور دچار مشکل می شوند را افزایش دهد.کارشناسان سمانتک می گویند این بدافزارها از خانواده بدافزارهایی موسوم به**Android.Reputation**.۱ هستند که اولین بار در سال ۲۰۱۴ از راه رسیدند.

این بدافزارها بعد از مدتی مخفی کاری فعالیت مخرب خود را آغاز کرده و ابتدا جلوی پاکسازی خود را می گیرند و سپس وب سایت های آلوده ای را به طور تصادفی در معرض دید کاربران قرار می دهند. هدف اصلی بدافزار یادشده کسب درآمد از کاربران پس از کلیک آنها بر روی صفحات این وب سایتهاست.بررسی ها نشان می دهد کدهای نگارش این بدافزار در مقایسه با سال ۲۰۱۴ تغییر چندانی نکرده و برنامه های ضدویروس عادی هم قادر به شناسایی و حذف کردن آن هستند.