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 ۹۶/۱۱/۱۱ شماره خبرنامه ۴۱۸

در این شماره می خوانید:

- بیت‌کوین
- تروجان‌ها
- ساعت‌های هوشمند
- بدافزار صوتی
- تدبیر مایکروسافت

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

وزنیاک همه بیت‌کوین‌هایش را فروخت

استیو وزنیاک از بنیانگذاران اپل اعلام کرد که بیت‌کوین همانند اعتیاد به مواد مخدر است و از این رو تمامی ارزهای دیجیتالی خود را فروخته است.به گزارش ایسنا، او افزود: در تابستان سال گذشته در بازار بیت‌کوین که قیمتی در حدود ۷۰۰ دلار داشت، سرمایه‌گذاری کردم، می‌خواستم این ارز را آزمایش کنم، با این حال هنگامی که بازار شروع به حرکت کرد و قیمت آن به محدوده ۲۰هزار دلار رسیده تمامی بیت‌کوین‌هایم را فروختم.

با ادامه روند افزایش بیت‌کوین تصمیم گرفتم تا به یکی از افرادی که روزانه اخبار ارزهای دیجیتال را دنبال می‌کند، تبدیل نشوم، من چنین نگرانی‌هایی را در زندگی‌ام نمی خواهم!ارز دیجیتال بیت کوین در ماه دسامبر در اوج قیمت به بیش از ۲۰ هزار دلار رسید اما از ابتدای ژانویه امسال با سقوط وحشتناک قیمت در محدوده ۱۰ هزار دلار معامله می شود.با این حال برخی از کشورها معاملات ارزهای دیجیتال را ممنوع کرده‌اند و در مقابل بازار ارزهای دیجیتال در سطح بین‌المللی بازار ارز همچنان با محبوبیت بالایی معامله می شود.

تروجان‌های آندروید صدای شما را ضبط می کنند

نرم افزارهای جاسوسی به تازگی با استفاده از قابلیت های نظارتی که دارند جایگاه خود را در فضای مجازی گسترش داده و باعث شده است دولت‌ها به این نوع نرم‌افزارها جذب شوند و آنها را خریداری کنند. نرم افزار جاسوسی **Skygofree** از ابتدای سال ۲۰۱۴ توسعه یافت و محققان آزمایشگاه کسپرسکی این نرم‌افزار را مورد تجزیه و تحلیل قرار داده‌اند و دریافتند که قابلیت این بدافزار با تروجان‌های اندرویدی دیگر تفاوت دارد.

محققان آزمایشگاه کسپرسکی گزارش نموده‌اند: «کاوشگر **Skygofree Android** یکی از قوی‌ترین ابزارهای جاسوسی است که ما تا به حال برای این پلتفرم دیده‌ایم.»با توجه به ویژگی‌های جدید نرم‌افزار **Skygofree** که در سال ۲۰۱۴ بدست آمده است عبارتند از: راه‌اندازی میکروفن آلوده برای ضبط صدا در یک مکان از پیش تعیین شده، سرقت پیام های **WhatsApp** و مجبور کردن سیستم عامل برای اتصال به شبکه **Wi-Fi** کنترل شده از سوی مهاجم.**Skygofree** توسط شرکت فناوری ایتالیایی نامعلوم تهیه شد که **HackingTeam** این نرم‌افزار جاسوسی را به برخی سازمان‌ها پیشنهاد فروش داده شده است.یکی از اهداف سازندگان بدافزار **Skygofree** ثبت دامنه به نام سایت‌های اپراتوراهای تلفن همراه به نام‌های **Vodafone، Three، Wind، Lycamobile** انجام گردید و این بدافزار با آلوده کردن سایتها، انتشار خود را گسترش داده‌اند.
این بدافزار، با سوءاستفاده از سیستم‌عامل‌های قدیمی که دانلودهای خود را از منابع نامشخص انجام می دهند هدف خود را اعمال نموده و سیستم را آلوده می کند.نسخه های پیشین **Skygofree** دارای ویژگی‌ها از قبیل آپلود فایل صوتی ضبط شده، سرقت و آپلود داده‌ها از کلیپ بورد و همچنین ضبط ویدئو و گرفتن عکس از دوربین جلویی گوشی که کاربر آن را اجرا می‌کند .

تحول در نمایشگر ساعت‌های هوشمند

شرکت هواوی به‌تازگی ثبت اختراع جدیدی را در رابطه با ساعت‌های هوشمند انجام داده است که می‌تواند قابلیت‌های جدیدی را –بدون نیاز به افزودن کلیدهای فیزیکی– به ساعت هوشمند یادشده بیفزاید. شرکت هواوی به‌تازگی ثبت اختراع جدیدی را در رابطه با ساعت‌های هوشمند انجام داده است که می‌تواند قابلیت‌های جدیدی را –بدون نیاز به افزودن کلیدهای فیزیکی– به ساعت هوشمند یادشده بیفزاید. بازار فناوری‌های پوشیدنی، به ویژه ساعت‌های هوشمند، پتانسیل زیادی برای رشد در اختیار دارد و بسیاری از شرکت‌ها برای بهبود عملکرد خود در این بازار تلاش می‌کنند، چرا که از نظر کارشناسان بازار، آینده اقتصادی خوبی در انتظار این عرصه است.در همین راستا نیز هواوی به‌تازگی اختراعی را به ثبت رسانده است که می‌تواند تحول بزرگی در صنعت ساعت‌های هوشمند این شرکت محسوب گردد.

اختراع یاد شده در واقع مربوط به ایجاد لبه‌هایی لمسی برای ساعت هوشمند است که در هشت ناحیه مختلف تقسیم شده و همین ویژگی، کاربری‌های زیادی را به ساعت‌های هوشمند می‌افزاید.این لبه‌های لمسی در واقع در کنار دکمه‌های متداول فیزیکی بالا و پایین، کارکردهای جدیدی از قبیل زوم کردن و ایجاد قابلیت‌های چرخشی دوانگشتی را برای کاربر به همراه دارد.

همچنین یکی از قابلیت‌های اصلی این اختراع در این است که می‌تواند بر روی همه نوع ماده اولیه متداول برای ساخت ساعت‌های هوشمند از قبیل پلاستیک، آلومینیوم، استیل ضدزنگ و... اجرا شود.لازم به ذکر است که هواوی واچ ۲ با اندروید پوشیدنی ۲.۰ را در کنفرانس جهانی موبایل سال ۲۰۱۷ میلادی رونمایی کرد و باید دید که آیا نسل سوم این ساعت‌های هوشمند با قابلیت یادشده به بازار عرضه خواهد شد یا خیر.

مراقب بدافزار صوتی، تصویری و ارز دیجیتال تلگرامی باشید

به تازگی بدافزار موبایلی با عناوین مختلف از جمله مکالمه تصویری تلگرام، مکالمه صوتی تلگرام و یا پول دیجیتال تلگرام، مکان‌یاب و ... از سوی مجرمین ایجاد گردیده که با آلوده کردن تلفن‌های همراه هوشمند اقدام به ارسال گسترده پیام برای مخاطبین قربانی می‌نماید. سرهنگ علی کریمی در گفت‌وگو با خبرنگار پایگاه اطلاع رسانی پلیس فتا اظهار کرد: با بررسی‌ها و رصد کارشناسان پلیس فتا استان کرمانشاه در آدرس این بدافزارها کلمه **telgram** مشاهده می‌شود که فیشینگ و جعلی بوده زیرا کلمه صحیح **telegram** می‌باشد.

وی تصریح کرد: این بدافزار ضمن دست‌کاری در اطلاعات اکانت تلگرام افراد قربانی برای تمامی مخاطبین فرد پیام ارسال می‌کند و آنان را ترغیب به نصب بدافزار می‌کند.این مقام ارشد انتظامی ادامه داد: با توجه به این‌که قربانی ابتدا پیام تبلیغاتی را از طریق دوستان خود دریافت می‌کنند باعث شده کاربر به موضوع اعتماد کرده و با نصب بدافزار در دام مجرم قرار گیرد.

وی با بیان اینکه این بدافزار ممکن است پس از نصب خود را مخفی نماید، در خصوص راه حذف آن گفت: برای حذف آن باید در قسمت تنظیمات گوشی بخش برنامه‌ها و حذف برنامه نصب شده اقدام کرد، در غیر این صورت به طور نامحدود به کار خود ادامه می‌دهد و امکان آسیب رساندن به اطلاعات، محتوا و سرقت شماره تلفن‌های فرد قربانی را داراست.سرهنگ کریمی تاکید کرد: از هموطنان عزیز درخواست داریم که به تبلیغاتی که برایشان ارسال می‌شود توجه نکنند و اگر قصد نصب برنامه‌ای را دارند حتما به ادرس آن توجه نماید.

تدبیر مایکروسافت برای آسیب‌پذیری‌ها

مایکروسافت قصد دارد با انتشار یک بروزرسانی نرم‌افزاری، رایانه‌های کاربران را از آسیب‌پذیری و ضعف امنیتی اسپکتر موجود در پردازنده اینتل محافظت کند. این ضعف‌ها و حفره‌های امنیتی در پردازنده‌های اینتل به‌گونه‌ای بوده است که به هکرها اجازه می‌داده علاوه بر سرقت کلمات و رمز عبور کاربران، تمامی اطلاعات ذخیره شده موجود بر حافظه، پردازنده رایانه و گوشی‌های همراه را به سرقت برده و از آن سوءاستفاده کنند و این سطح از دسترسی موجب می‌شد به تراشه‌های دیگری همچون ای.ام.دی و ای.آر.ام نیز دسترسی یابند.

اینتل، یک شرکت تجهیزات رایانه‌ای در ایالات متحده آمریکاست که در زمینه تولید سخت‌افزارهای رایانه و تلفن همراه، با تمرکز بر مادربورد، کارت شبکه، چیپ‌ست، بلوتوث و حافظه‌های فلش، انواع ریزپردازنده، نیم‌رسانا، مدارهای مجتمع، واحدهای پردازش گرافیکی و سامانه‌های نهفته فعالیت می‌کند.پس از آنکه خود اینتل نیز پس از ارائه و انتشار بروزرسانی ویژه‌ای برای جلوگیری از آسیب رسیدن به رایانه‌های کاربران، به آنها هشدار داد که از این بروزرسانی استفاده نکرده و آن را به هیچ وجه بر روی سیستم عامل رایانه خود نصب نکنند، حالا شرکت مایکروسافت در قبال این خطر و تهدید بزرگ احساس مسئولیت کرده و تصمیم گرفته است که به زودی در یک بروزرسانی نرم افزاری، کاربران سیستم عامل ویندوز را از یکی از آسیب‌پذیری‌های بزرگ و معروف اینتل یعنی اسپکتر محافظت کند. مایکروسافت در تشریح این موضوع اعلام کرده است که قصد دارد برای سیستم عامل‌های ویندوز ۷، ویندوز ۸.۱ و ویندوز ۱۰ یک بروزسانی منتشر کند تا آنها را از خطر سواستفاده و سرقت اطلاعات ضعفهای امنیتی اسپکتر برهاند.

استیضاح بزرگترین مرکز مبادلات بیت‌کوین در ژاپن

مرکز مبادلات ارز دیجیتالی کوین چک ژاپن پس از آنکه هکرها ۵۳۰ میلیون دلار از آن را به سرقت بردند، توسط رگولاتورهای مالی ژاپن استیضاح شد.این روزها که بازار ارزهای دیجیتالی رمزنگاری شده بسیار داغ شده است، وب‌سایت‌ها، حساب‌های کاربری و پلت‌فرم‌های بسیاری برای استخراج بیت‌کوین یا بیت‌کوین ماینینگ ایجاد شده است تا بتوانند با استفاده از آنها به خرید و فروش و مبادلات تجاری کلان اقدام کنند.

دو روز پیش بود که هکرها به یکی از بزرگ‌ترین مراکز مبادلات ارز دیجیتالی رمزنگاری شده در ژاپن نفوذ و حمله کرده و ۵۳۲ میلیون دلار را به سرقت بردند.کوین چک – یکی از بزرگ‌ترین مراکز مبادلات ارز دیجیتالی رمزنگاری شده است که در شهر توکیوی ژاپن مستقر شده – اعلام کرد که هکرها و مجرمان سایبری با نفوذ و حمله به سرورهای این مرکز، ۵۳۲ میلیون دلار از سرمایه‌هایش را به سرقت برده‌اند.

این مرکز در تشریح بزرگترین هک و حمله سایبری که در معرض آن قرار گرفته اعلام کرده است که ۴۲۰ میلیون دلار از ارز دیجیتالی **NEM** و ۱۱۲ دلار نیز از ارز دیجیتالی ریپل توسط هکرها ربوده شده و این شرکت را در آستانه ورشکستگی قرار گرفته است.حالا مراکز و رگولاتورهای مالی در کشور ژاپن این مرکز مبادلاتی ارز دیجیتالی را استیضاح کرده و از مدیران و مسئولان مربوطه آن درخواست کرده اند که در این خصوص توضیحات بیشتر و دقیق‌تری بدهند چراکه آنها بر این باورند که اگر متخصصان امنیت سایبری به خوبی و سریع، هک و حمله سایبری مذکور را شناسایی می‌کردند، مبلغ به سرقت برده شده توسط هکرها آنقدر زیاد نمی شد. در سال ۲۰۱۴ میلادی هم یکی از بزرگ‌ترین مراکز مبادلاتی بیت کوین در آن زمان، پس از آنکه ۴۵۰ میلیون دلار از سرمایه‌هایش را از دست داد، اعلام ورشکستگی کرد. بنابراین بسیاری از تحلیلگران معتقدند که کوین چک نیز همانند برخی دیگر از موسسات و مراکز دیگر با از دست دادن چنین مبلغ هنگفتی رو به ورشکستگی خواهد رفت.بسیاری از کشورهای جهان از جمله کشورهای اروپایی درتلاش هستند تا این پول بی‌افسار را کنترل کرده و معاملات با آن را تا حد امکان محدود کنند، چرا که آنها بر این باورند بیت‌کوین به تجارت‌های غیرقانونی و غیرمجاز همچون تجارت اسلحه، تجهیزات تروریستی، قاچاق دارو و موادمخدر دامن‌زده و به علت آنکه مقامات قضایی و پلیس نمی‌توانند طرفین معامله را شناسایی و ردگیری کنند، باعث سهولت آن می‌شود.