«کرونا» بزرگترین عامل کلاهبرداری آنلاین در جهان

میترا جلیلی
خبرنگار

شیوع کرونا باعث افزایش انفجاری حملات فیشینگ و فریب کاربران شده است به‌گونه‌ای که غول‌های دنیای فناوری معتقدند کووید۱۹ را می‌توان بزرگ‌ترین موضوع کلاهبرداری‌های آنلاین جهان دانست. طبق تازه‌ترین گزارش گوگل، سرویس جیمیل با بیش از ۱.۵میلیارد کاربر، بزرگ‌ترین بستر برای کلاهبرداران اینترنتی محسوب می‌شود چراکه گوگل در تازه‌ترین گزارش خود از مسدودسازی روزانه ۱۰۰میلیون ایمیل فیشینگ در هفته های اخیر خبر داده و یادآور شده است که حدود یک پنجم آنها مرتبط با کروناویروس بوده‌اند. اما کاربران در گوشه و کنار جهان چقدر از این کلاهبرداری‌های آنلاین متضرر شده اند؟

■ افزایش ۶۶۷درصدی فیشینگ در بریتانیا

اسکمرها (کلاهبرداران اینترنتی) روزانه ۱۸میلیون ایمیل فریبنده درباره کروناویروس را برای کاربران ارسال می‌کنند تاجایی که این افزایش کلاهبرداری‌های آنلاین، واکنش مراکز مختلف سایبری جهان را به‌دنبال داشته است. بریتانیا یکی از کشورهایی است که از کلاهبرداری‌های آنلاین دوران کرونا درامان نمانده است و در همین راستا بخشی با عنوان مرکز امنیت ملی سایبری بریتانیا(NCSC) که یک سرویس گزارش ایمیل است، راه‌اندازی کرده تا عموم مردم بتوانند هرگونه فعالیت مشکوک را ردیابی و پرچمدار کنند زیرا به این ترتیب، هم یافتن اسکمرها برای این مرکز راحت‌تر می شود و هم تعداد کمتری از کاربران فریب می خورند.

رشد فیشینگ با موضوع کروناویروس توسط بسیاری از کمپانی‌های امنیت سایبری تأیید شده است و به‌عنوان مثال کمپانی Barracuda Networks از افزایش ۶۶۷درصدی ایمیل‌های فیشینگ در جریان شیوع گسترده کرونا در بریتانیا خبر داده است. (فیشینگ به تلاش برای به‌دست آوردن اطلاعات خصوصی کاربر ازطریق جعل وبگاه، آدرس ایمیل و... گفته می‌شود.) این حملات سایبری تنها ازطریق ایمیل انجام نمی‌شود وبرخی اپلیکیشن‌های تلفن‌های هوشمند و وب سایت‌های مخرب هم در این بخش فعال هستند و به‌عنوان مثال با فریب کاربر با عنوان ردیابی شیوع کرونا از طریق اپ، عملاً گوشی کاربر را به باج افزار آلوده می‌کنند و درخواست باج می‌کنند تا اطلاعات را به کاربر پس بدهند.

تازه‌ترین گزارش Action Fraud مرکز گزارش کلاهبرداری و جرایم سایبری بریتانیا نیز نشان می‌دهد همزمان با کرونا و سوءاستفاده مجرمان سایبری از شیوع کووید۱۹، دراین کشور بیش از ۲میلیون پوند ازطریق فیشینگ ایمیل، اسکم و سایر روش‌های کلاهبرداری‌های آنلاین در بریتانیا به سرقت رفته است. در این گزارش آمده است هزینه کل ۸۶۲مورد اسکم که تا روز ۱۷ آوریل در بحران کرونا صورت گرفته، ۲میلیون و ۱۲۰هزار و ۸۷۰ پوند بوده است. این مرکز همچنین در این مدت درمجموع بیش از ۳هزار و ۶۰۰ گزارش و شکایت فیشینگ ایمیل مرتبط با کروناویروس را از کاربران دریافت کرده است. هدف این حملات، فریب کاربران برای دسترسی به اطلاعات شخصی کاربر و جزئیات اطلاعات بانکی آنها ازطریق کلیک بر ایمیل‌هایی با لینک‌های آلوده است.

طبق گزارش مرکز Action Fraud بیشتر اسکم‌ها در بریتانیا مربوط به فروش آنلاین وسایل حفاظتی کرونا هستند که مردم با کمبود آن مواجهند. این مرکز به مردم هشدار داده که قبل از خرید نگاهی به تاریخچه فعالیت سایت داشته باشند و بی‌گدار به آب نزنند.Action Fraud همچنین یادآور شده است نه پلیس و نه دولت هرگز تقاضای جابه‌جایی پول یا استفاده از بیت‌کوین یا هر ارز مجازی دیگری نخواهند داشت و کاربران اینترنت نباید نسبت به لینک‌های مشکوک در قالب ایمیل واکنشی نشان بدهند.

■ آسیب پذیرترین‌های امریکا در تیررس اسکمرها

بسیاری از امریکایی‌ها نیز در بحران کرونا آسیب پذیر شده‌اند. به‌دلیل شیوع ویروس کووید۱۹میلیون‌ها نفر بیکار شده‌اند و البته اسکمرها نیز این دردسرها را تشدید کرده‌اند. به‌تازگی کمیسیون تجارت فدرال ایالات متحده اعلام کرده است که کاربران امریکایی در سه ماهه نخست سال‌جاری میلادی حدود ۱۸هزار مورد شکایت در زمینه کلاهبرداری‌های آنلاین به این کمیسیون ارائه داده و در بحران کرونا بیش از ۱۳.۴میلیون دلار را از دست داده‌اند.

در امریکا انواع اسکم‌ها (کلاهبرداری ها) دیده می‌شود که یکی از آنها اسکم‌های درمانی هستند. این اسکمرها با معرفی خود به‌عنوان پزشک، وانمود می‌کنند یکی از صمیمی‌ترین دوستان شما درحال درمان کرونا در بیمارستان است و از شما می‌خواهند مبلغی را به حساب بیمارستان واریز کنید. برخی کلاهبرداران اینترنتی نیز بیشتر سراغ افراد آسیب پذیرتر به کرونا می‌روند و با معرفی داروی قطعی کرونا یا ارائه کیت‌های تشخیصی رایگان برای دیابتی‌ها، کاربران را فریب می‌دهند. برخی دیگر در قالب خیریه‌ها سازماندهی شده‌اند که بسیار شبیه گروه‌های مورد تأیید سازمان جهانی بهداشت هستند. کاربران با ثبت‌نام در لینک جعلی ارسال شده توسط این گروه‌ها به محض تلاش برای اهدای کمک‌های نقدی، تمام اطلاعات بانکی‌شان را در معرض سرقت قرار می‌دهند.

سی‌ان‌ان

برخی اسکمرها نیز افرادی را نشانه می‌گیرند که شغل خود را از دست داده‌اند. به‌عنوان مثال کمیسیون ارتباطات فدرال امریکا(FCC) در گزارشی خبر داده که بسیاری از امریکایی‌ها ایمیلی از مرکز مراقبت‌های مالی FCC دریافت کرده‌اند که حاوی پیشنهاد کمک ۳۰هزار دلاری برای کمک به کسانی است که تحت تأثیر COVID-19 قرار گرفته‌اند درحالی که چنین برنامه‌ای وجود ندارد و این ایمیل‌ها تنها راهی برای فریب کاربران در تهیه اطلاعات شخصی هستند.

■ سوءاستفاده از کمک‌های مالی در آلمان

آلمان هم این روزها از کلاهبرداران آنلاین در امان نمانده و کاربران از طریق دریافت ایمیل‌های آلوده با موضوع هشدارهایی درباره کرونا یا اخبار مربوط به درمان بیماری و فیشینگ، ده‌ها میلیون یورو از دست داده‌اند که این موضوع در یکی از استان‌های غربی این کشور نمود بیشتری دارد. مجرمان سایبری در استان نورت راین وستفالیای آلمان (NRW) نسخه‌های کپی از یک وب سایت رسمی مربوط به وزارت امور اقتصادی این کشور را ایجاد کردند. وب سایت اصلی برای توزیع کمک‌های مالی COVID-19 راه‌اندازی شده است و به‌همین دلیل هم روزانه کاربران زیادی به آن مراجعه می‌کنند. در این بین تعدادی بدون توجه به اصالت وب سایت، به نسخه کپی مراجعه کرده‌اند و اطلاعاتشان توسط هکرها استخراج شده است.

کلاهبرداران با استفاده از این اطلاعات، لینک‌هایی از طریق ایمیل برای کاربران ارسال می‌کنند و آنها را فریب می‌دهند. آنها سپس به نمایندگی از کاربران واقعی درخواست کمک‌های دولتی می‌کنند و وجه، به حساب آنها واریز می‌شود. یعنی عملاً نام کاربر در لیست کسانی قرار می‌گیرد که کمک دریافت کرده‌اند ولی عملاً جیب آنها خالی است و هیچ پولی عایدشان نمی‌شود.

پلیس NRW در طول یک هفته ۵۷۶ شکایت رسمی در این زمینه دریافت کرد. گفتنی است دولت آلمان در این استان بیش از ۳۸۰هزار تقاضای کمک دریافت کرد که با تقاضای ۳۶۰هزار نفر آنها موافقت اعلام شد. در این میان به‌نظر می‌رسد ۳هزار و ۵۰۰ تا ۴هزار تقاضا غیرواقعی و کلاهبرداری باشد. گفتنی است کمک‌های مالی از ۹هزار یورو برای کسب و کارهای مستقل تا ۲۵هزار یورو برای کمپانی‌هایی با بیش از ۵۰ کارمند را شامل می‌شود. به این ترتیب تخمین زده می‌شود دولت در طول بحران کرونا حداقل ۳۱.۵میلیون یورو معادل ۳۴.۲۵میلیون دلار و حداکثر ۱۰۰میلیون یورو معادل ۱۰۹ میلیون دلار به کلاهبرداران پرداخت کرده است.

■ این تروجان‌های خطرناک در ایتالیا

در ایتالیا نیز کلاهبرداران اینترنتی بسیار فعال هستند و هرچند هنوز رقمی که کاربران در اثر این حملات سایبری از دست داده‌اند مشخص نشده ولی مطمئناً رقم کمی نیست چراکه اسکمرها از وضعیت وخیم و ترس کاربران نهایت استفاده را برده‌اند و آنها را بیش از همه با دو بدافزار Trickbot و Lokibot مورد حمله قرار داده‌اند.

«چستر ویسینوسکی» از محققان مؤسسه امنیت سایبری Sophos در ایتالیا معتقد است که Trickbot یک تروجان بانکداری است که پیش از این نیز برای سرقت اطلاعات محرمانه حساب‌های بانکی کاربران به کار می‌رفت اما در دوران کرونا در ایتالیا بسیار پرکارتر شده است. مجرمان سایبری ماهری که پشت این هک‌ها قرار دارند، کاربران نگران از ویروس کووید ۱۹ را به راحتی شکار کرده و با ایمیل تقلبی آنها را فریب می‌دهند. محققان و تحلیلگران این مؤسسه به مردم سایر نقاط دنیا نیز هشدار داده‌اند و معتقدند با اینکه این بدافزار اکنون در ایتالیا فعالیت گسترده‌ای دارد ولی اوضاع به همین منوال پیش نمی‌رود و احتمالاً این بدافزار در سایر نقاط جهان نیز کاربران مستأصل را شکار خواهد کرد.Lokibot نیز تروجان دیگری است که این روزها رد پای آن در ایتالیا زیاد دیده می‌شود. این بدافزار عملاً یک درپشتی در سیستم ویندوز ایجاد می‌کند تا اطلاعات حساس و شخصی قربانیان ازجمله رمز عبور، نام کاربری و جزئیات حساب‌های بانکی آنها را با کمک یک keylogger به سرقت ببرد.

ساعت های هوشمند خورشیدی در راه بازار

صهبا ملک / محقق

سلول‌های خورشیدی ویژه و قابل انعطافی طراحی کرده‌اند که می‌توانند در آینده، فناوری‌های پوشیدنی بسیار تأثیرگذار باشد. این سلول‌های خورشیدی ۱۰ بار باریک‌تر از موی انسان هستند و تنها ۳دهم میکرومتر قطر دارند. این سلول‌های خورشیدی آنقدر سبک هستند که می‌توان آنها را روی گلبرگ‌های گل قرار داد. موضوع مهم دیگر این است که این سلول خورشیدی در عین سبک بودن، بسیار قدرتمند است و می‌تواند به ازای هرگرم وزن خود ۹.۹ وات انرژی تولید کند. این بدان معناست که می‌توان با استفاده از آن، انرژی مورد نیاز یک ساعت مچی هوشمند را به راحتی تأمین کرد. شاید در آینده روزی فرا برسد که هیچ یک از ساعت‌های هوشمند خورشیدی نیازی به باتری نداشته باشند. این موضوع می‌تواند خبر خوشی برای دوستداران محیط زیست باشد چراکه باتری‌ها بخش زیادی از زباله الکترونیک جهان را به‌خود اختصاص می‌دهند و حذف آنها می‌تواند کمک بزرگی به کره زمین باشد.

این تکنولوژی می‌تواند کمک کند تا وسایل دیجیتال بویژه فناوری‌های پوشیدنی مدت زمان زیادی بدون نیاز به شارژ الکتریکی کار کنند. نتایج آزمایش‌های اولیه نشان می‌دهد که این سلول خورشیدی که به‌جای باتری در ساعت هوشمند کار گذاشته می‌شود پس از ۴هزار و ۷۰۰ساعت کار کردن تنها ۴.۸ درصد آثار کهنگی در آن دیده می‌شود و تا ۲۰هزار ساعت که کار کرده باشد هنوز آثار فرسودگی چندانی روی آن دیده نمی‌شود بنابراین عمر مفید این سلول‌های خورشیدی به طور متوسط ۱۱.۵ سال است که رقم مناسبی برای یک باتری محسوب می‌شود.

البته درحال حاضر انرژی که این باتری کوچک می‌تواند تولید کند تنها برای وسایل و فناوری‌های کوچک پوشیدنی ازجمله ساعت یا دستبندهای هوشمند کارآیی دارد و برای وسایل بزرگ‌تر احتمالاً یا باید این سلول را در ابعادی بزرگ‌تر طراحی کرد یا اینکه به‌گونه‌ای، سطح آن را بیشتر در معرض نور خورشید قرار داد تا انرژی بیشتری تولید کند. این سلول خورشیدی در حال حاضر می‌تواند تا ۱۳درصد انرژی خورشیدی تولید کند. این رقم نسبت به سلول‌های خورشیدی معمولی که بیش از ۲۰درصد انرژی خورشیدی تولید می‌کنند چندان زیاد نیست هرچند می‌تواند انرژی ساعت‌های هوشمند را تأمین کند. البته باید برای ساخت این سلول خورشیدی از فناوری پرینت سه بعدی تشکر کرد چراکه شاید اگر این فناوری نبود هنوز نمی‌توانستیم شاهد طراحی و تولید چنین سلول‌های خورشیدی باشیم. البته باید گفت که محققان در انتظار فرصتی هستند تا فناوری این سلول خورشیدی را تجاری‌سازی کنند هرچند غالباً چندین سال طول می‌کشد تا چنین طرح‌هایی به مرحله تولید انبوه برسد. البته پیش از این نیز از سلول‌های خورشیدی برای ساعت‌های هوشمند استفاده شده ولی این نخستین بار است که قرار شده در ساعت هوشمند آینده، هیچ باتری یدکی هم وجود نداشته باشد. پیش از این کمپانی ماتریکس به این بخش وارد شده و ساعت هوشمندی ارائه داده بود که هم ضربان قلب را می‌تواند اندازه‌گیری کند و هم مجهز به جی‌پی‌اس است و با سلول خورشیدی کار می‌کند اما یک باتری یدکی هم دارد.

نرم افزار آنلاین

چگونه بدافزار های تبلیغاتی را حذف کنیم؟

اگر شما جزو افرادی هستید که از شبکه های اجتماعی یا سایت ها استفاده می کنید حتماً برای شما هم پیش آمده که از تبلیغات متعدد آنلاین کلافه شده اید. بیشتر این تبلیغات تنها جنبه تجاری دارند و می خواهند مشتری جذب کنند اما باید گفت که گاهی هم این تبلیغات آنلاین عملاً بدافزارهایی خطرناک هستند و می توانند حریم خصوصی شما را به خطر بیندازند یا سبب خالی شدن حساب های بانکی تان شوند. به همین دلیل نصب نرم افزارهای مقابله با این تبلیغات کمک شایان توجهی به شما خواهد کرد.

یکی از این نرم افزارها Ultra Adware Killer است؛ یک نرم افزار حرفه ای و ویژه برای حذف بدافزارهای تبلیغاتی که کارآیی بالایی دارد. با استفاده از این نرم افزار بسیار ساده اما پرقدرت، امنیت سیستم شما به صورت کامل حفظ شده و از ورود بدافزارها به سیستم تان جلوگیری می شود و باعث بهبود کارایی سیستم می شود. این

نرم افزار از ورود و اجرای تبلیغات ناخواسته تولبارهای تبلیغات، پلاگین های تبلیغاتی، نمایش نتایج ناخواسته در جست وجوها و... جلوگیری می کند. به این ترتیب با خیالی راحت تر می توانید در اینترنت به جست و جو بپردازید.

همچنین از دیگر ویژگی های این نرم افزار قابلیت ریست کردن مرورگرهای کروم و فایرفاکس به تنظیمات پیش فرض است. Ultra Adware Killer نرم افزاری سبک وبسیار سریع با کارایی دقیق برای جلوگیری از اجرای پاپ آپ ها به شمار می رود و برای اجرا و کار با این نرم افزار کافی است دکمه استارت را بزنید و صبر کنید تا کار اسکن تمام شود و بعد از اتمام اسکن، موارد یافت شده را پاک کنید. با کمک این نرم افزار احتمال حمله بدافزارها به سیستم تان بسیار پایین می آید و می توانید مطمئن تر از گذشته در فضای آنلاین به جست و جو بپردازید.

به هرحال اگر شما هم علاقه دارید که این نرم افزار را در اختیار داشته باشید و از دست بدافزارهای تبلیغات و همچنین تبلیغات گاه و بیگاه آنلاین در هنگام جست و جو در اینترنت در امان بمانید می توانید آن را به طور رایگان از سایت P30world.com بارگذاری کنید.

قاب فناوری

توپ هوشمند برای بازیکنان راگبی

علیرضا احمدی / راگبی یکی از بازی‌های پرطرفدار در جهان محسوب می شود اما یکی از بزرگ‌ترین مشکلات آن، چالش‌های داوری مسابقات آن است. در همین راستا فعالان حوزه فناوری برای رفع این مشکل دست به کار شده و توپ هوشمند راگبی را ارائه داده‌اند.

این توپ هوشمند مجهز به تعدادی سنسور است و می تواند همه حرکات بازیکنان را ثبت کند تا اگر در طول بازی خطایی انجام شد، داور به راحتی بتواند خطا را بگیرد. سخت افزار به کار رفته در ساخت این توپ، توسط کمپانی بریتانیایی Sportable تولید شده و خود توپ هم توسط شرکت Gilbert طراحی شده است. برخی از سنسورهای این توپ هوشمند شتاب سنج، مغناطیس سنج و ژیروسکوپ هستند و برخی نیز سنسورهای حساس به دما محسوب می شوند. این سنسورها و سایر ابزارهای به کار رفته در این توپ هوشمند، اطلاعاتی همچون موقعیت

و نحوه چرخش توپ، فاصله و ارتفاع طی شده توسط توپ، توقف توپ و... را جمع آوری می کند. این اطلاعات توسط تکنولوژی RFID منتقل می شود. درواقع هر بازیکن یک برچسب RFID روی لباسش چسبانیده شده بنابراین تمام حرکات آنان در طول بازی قابل ردیابی است به همین دلیل هم در بازی پربرخورد راگبی هرگونه خطا کاملاً قابل شناسایی است.

گفته می‌شود مربیان نیز می توانند از امکانات این توپ هوشمند بیشترین بهره را بگیرند و میزان آمادگی بازیکنان خود را محک بزنند. به عنوان مثال مربی می تواند مدت زمانی که یک توپ پس از شوت بازیکن در هوا باقی می ماند، شدت ضربه به توپ و... را اندازه گیری کند. این توپ سال گذشته به صورت آزمایشی در تورنمنت RugbyX لندن مورد استفاده قرار گرفت و داوران و برگزارکنندگان این مسابقه از عملکرد آن رضایت داشتند هرچند ایراداتی نیز به آن وارد می دانستند. این مسابقه به دلیل سرعت بالا، یکی از بهترین میادین برای آزمایش این توپ هوشمند به شمار می رفت. حالا با رفع مشکلات این توپ هوشمند، قرار است این وسیله پرکاربرد در اختیار تیم های ورزشی قرار بگیرد. البته پیش از این نیز شاهد طراحی و تولید توپ های هوشمند برای فوتبال، بسکتبال، بیسبال نیز بوده ایم اما هیچ یک به هوشمندی این توپ جدید راگبی نبوده‌اند.

اخبار

ساخت نمونه تجاری «سار هواپایه» در پژوهشگاه فضایی

رئیس پژوهشگاه فضایی ایران با اشاره به اهداف تجاری‌سازی دستاوردهای فضایی گفت: نمونه تجاری سامانه سار هواپایه با کاربردهایی در حوزه‌های مدیریت حوادث غیرمترقبه، نقشه‌برداری، کنترل مرزها در پژوهشکده مکانیک پژوهشگاه فضایی ایران در شیراز طراحی و ساخته شد.

به‌گزارش «ایران»، حسین صمیمی با بیان اینکه رادار دهانه مصنوعی (سار) نوعی از رادار است که بر سکوهای متحرکی مثل هواپیما، پهپاد و ماهواره نصب می‌شود، گفت: در هنگام حرکت سکو، رادار با ارسال متناوب پالس به سطوح و دریافت بازگشتی آن، قادر است تصویری دقیق از ناحیه هدف را ایجاد کند. صمیمی با اشاره به مزایای عمده تصویربرداری راداری نسبت به تصویربرداری اپتیکی تصریح کرد: قابلیت تصویربرداری از پشت ابر و در تمام ساعات شب و روز (مستقل از نور خورشید) و حتی نواحی پوشیده شده از دود و گرد وخاک، مستقل بودن کیفیت تصویر راداری از فاصله، امکان کشف اهداف یا اشیای فلزی استتار شده از مزایای این رادار است.

وی افزود: مزایای عمده تصویربرداری سار نسبت به تصویربرداری اپتیک، باعث توجه روزافزون همه کشورهای توسعه یافته به این فناوری شده و در دهه‌های اخیر، در این کشورها سرمایه‌گذاری هنگفتی در صنعت سار صورت گرفته است و فناوری آن را به انحصار خود درآورده‌اند.

صمیمی با اشاره به اینکه طراحی، ساخت، آزمون و بهره‌برداری از این رادار تصویربرداری هواپایه حاصل تحقیقات و تلاش شبانه‌روزی نخبگان علمی و فنی پژوهشگاه فضایی ایران است، گفت: این سامانه به علت دستیابی به کیفیت بالا در استخراج تصاویر، قادر است بخش زیادی از نیازمندی کشور در این زمینه را برطرف سازد.

وی درباره تجاری‌سازی این پروژه اظهار کرد: پس از ساخت و آزمون نمونه مهندسی این سامانه در سال ۱۳۹۶ در پژوهشکده مکانیک و انجام آزمون‌های پروازی موفق، طراحی و ساخت نمونه تجاری این سامانه، با هدف تجاری‌سازی دستاوردهای فضایی، در دستور کار این پژوهشگاه قرار گرفت.

۱۱هزار کیلومتر روایت تاریخی دیجیتال در حال شکل گیری

سازمان فناوری اطلاعات، وزارت میراث فرهنگی، اپراتورها و پلتفرم‌ها در همکاری با یکدیگر قرار است ۱۱ هزار کیلومتر روایت تاریخی را به شیوه دیجیتال در دسترس کاربران قرار بدهند؛ این روایت تاریخی از اهواز آغاز خواهد شد.

به‌گزارش ایرنا، امیر ناظمی رئیس سازمان فناوری اطلاعات دراین خصوص گفت: هر روز یک ساعت از این روایت تاریخی ۱۱هزار کیلومتری میراث‌های فرهنگی، از طریق پلتفرم‌هایی که در این پروژه مشارکت دارند پخش می‌شود. روایت دیجیتالی این مسیر به شکل‌گیری همکاری خوبی بین دولت و بخش خصوصی منجر شده است.

معاون وزیر ارتباطات درباره چرایی انجام این کار افزود: کرونا چالش سخت جهانی است که در برخی موارد منجر به خلاقیت شده است. در ایام عید برنامه بازدید آنلاین از موزه‌ها را به شکل پایلوت به مرحله اجرا درآوردیم. در این مدت پخش مستقیم از ۳۰۰ موزه را انجام دادیم. این کار بیش از برآورد ما مورد استقبال قرار گرفت. به‌همین دلیل تصمیم گرفتیم آن را ادامه بدهیم و به‌کارهای بزرگ‌تر فکر کنیم.

درخواست فرانسه از اپل برای توسعه برنامه ردیابی

فرانسه از اپل خواسته است که موانع فنی موجود بر سر راه توسعه برنامه ردیابی مستقیم را که برای مدیریت و نظارت بر شیوع کووید۱۹ طراحی شده است، از میان بردارد.

به گزارش ایسنا، این برنامه که مشابه برنامه‌هایی است که هم‌اکنون توسط شرکت‌های اپل و گوگل توسعه یافته و به بخشی از زندگی روزمره مردم چین تبدیل شده است، برای کمک به بخش‌های خدمات درمانی ساخته شده است تا تعیین کنند که افراد آلوده و مبتلا با چه کسانی در تماس بوده‌اند و به دولت‌ها در تصمیم‌گیری در مورد کاهش محدودیت‌های جابه‌جایی و اجتماعی کمک می‌کند. این برنامه که برای راه‌اندازی در فرانسه از تاریخ ۱۱ ماه مه توسعه یافته است، به فناوری بلوتوث متکی است، اما سیستم عامل اپل (iOS) اگر داده‌های به‌دست آمده از دستگاه منتقل شود، اجازه نمی‌دهد بلوتوث در حالت پس زمینه اجرا شود.

در حالی که این اقدامی است که برای محافظت از حریم شخصی کاربران توسط اپل طراحی شده است، اما اکنون در شرایط همه‌گیری کرونا به نوعی این محافظت از حریم شخصی افراد باعث شده امکان ردیابی و نظارت بر شیوع آن برای فرانسه سلب شود.

«سدریک او»، وزیر دیجیتال فرانسه در گفت‌وگو با بلومبرگ گفت: ما از شرکت اپل می‌خواهیم که موانع فنی را برطرف کند تا به ما اجازه دهد یک راه حل عالی بهداشتی برای اروپا تهیه کنیم که به سیستم بهداشتی ما گره بخورد.

با این حال به نظر می‌رسد اپل پذیرای این درخواست نخواهد بود و درعوض به توسعه برنامه مشابه خود با همکاری گوگل می‌پردازد.

این درخواست با توجه به مسائل بالقوه‌ای که برای حریم خصوصی مرتبط با این نوع برنامه‌ها به‌وجود می‌آورد، موضوع گسترده‌تری را برجسته می‌کند. اتحادیه آزادی‌های مدنی امریکا(ACLU) به‌تازگی یک مقاله طولانی منتشر کرده است که نگرانی‌های پیرامون فناوری ردیابی مستقیم که باید در نظر گرفته شود، ذکر می‌کند.

«جنیفر استیسا گرانیک»، مشاور نظارت و امنیت ACLU نوشت: در حالی که برخی از این برنامه‌ها می‌توانند بهداشت عمومی را ارتقا دهند، اما ممکن است خطرات قابل توجهی برای حریم خصوصی، حقوق شهروندی و آزادی‌های مدنی ایجاد کنند.

فروش اطلاعات ۲۶۷ میلیون کاربر فیس بوک در وب تاریک

محققان امنیتی اعلام کرده‌اند اطلاعات ۲۶۷ میلیون حساب کاربری فیس‌بوک در وب تاریک به قیمت فقط ۶۰۰ دلار فروخته شده است.

به‌گزارش مهر و طبق گزارش محققان شرکت امنیت سایبری Cyble میلیون‌ها حساب کاربری فیس‌بوک که حاوی اطلاعات شخصی است در وب فروخته شده است. این اطلاعات شامل نام و نام خانوادگی، آدرس ایمیل، شماره تماس، آی‌دی فیس‌بوک و غیره است.

محققان این شرکت خرید اطلاعات را تأیید کردند. همچنین آنها مخزنی از اطلاعات مذکور برای کاربران ایجاد کردند تا بتوانند وجود اطلاعات خود در منابع سرقت شده را بررسی کنند. این مخزن اطلاعاتی در .AmlBreached com وجود دارد. هرچند در این عملیات هک اطلاعات حساسی مانند پسوردها فاش نشده، اما هکرها با داده‌های موجود می‌توانند از مردم سراسر جهان کلاهبرداری کنند. در پست وبلاگی محققان آمده است: ما هنوز نمی‌دانیم اطلاعات چگونه فاش شده است، اما احتمال می‌دهیم دلیل این امر افشای APIهای طرف سوم باشد.