دانش

آمریکا ویروس بیماری کووید-۱۹را ساخته است؟

فرضیه بروز ویروس SARS-CoV-2 عامل بیماری کووید-۱۹ از یک آزمایشگاه در آمریکا از ابتدای شروع همه‌گیری مطرح بود. برخی از متخصصان این ویروس را ویروس دست‌ساز انسانی می‌دانند و به اعتقاد آنها ریشه طبیعی ندارد. در شبکه‌های مجازی نیز اخیرا از قول جفری ساکس، استاد دانشگاه کلمبیا، ادعایی مبنی بر ساخت این ویروس در آزمایشگاه و انتشار عمدی آن شده است. پروفسور جفری ساکس اعلام کرده که تقریبا مطمئن شده که این ویروس منشأ طبیعی ندارد. ما در طول زندگی بارها با ویروس‌هایی از خانواده کرونا به واسطه ابتلا به آنفلوآنزا و سرماخوردگی برخورد داشته‌ایم. اما نوع جدید ویروس کرونا که بیش از ۲سال زندگی جهانیان را مختل کرده است، بسیار مرموز و ناشناخته بود. زمانی که جو بایدن، رئیس‌جمهور آمریکا از جامعه اطلاعاتی ایالات متحده (IC) خواست تا منشأ کووید-۱۹ را مشخص کند، نتیجه به‌طور عجیبی تکان‌دهنده بود. IC به روشنی اعلام کرد، نمی‌تواند این احتمال را که SARS-CoV-2 از یک آزمایشگاه بیرون آمده باشد، رد کند. حتی بدتر از این، اگر ویروس واقعا نتیجه تحقیقات و آزمایش‌های آزمایشگاهی باشد، تقریبا به‌طور قطع با بیوتکنولوژی و دانش آمریکا ایجاد و منتشر شده است.

برای دانستن حقیقت کامل در مورد منشأ کووید-۱۹، یک تحقیق کامل و مستقل نیاز است. اگر ویروس از آزمایشگاه بیرون آمده باشد، تقریبا می‌توان گفت به‌طور تصادفی در روند عادی تحقیقات این کار انجام شده است و احتمالا از طریق عفونت بدون علامت قابل شناسایی و پیشگیری نبوده است. البته هنوز هم ممکن است که ویروس منشا طبیعی داشته باشد. نکته اصلی این است که هیچ‌کس واقعیت را نمی‌داند. به همین دلیل است که بررسی تمام اطلاعات مرتبط موجود در پایگاه‌های داده موجود در آمریکا بسیار مهم است. از زمان شروع همه‌گیری در اوایل سال ۲۰۲۰، دولت آمریکا انگشت اتهام را به سمت چین نشانه رفته است. درست است که نخستین موارد مشاهده شده کووید-۱۹ در ووهان بوده، اما داستان کامل شیوع درصورتی که به‌طور قطع روشن شود، می‌تواند نقش آمریکا را در تحقیق در مورد کرونا و به اشتراک گذاشتن بیوتکنولوژی خود با دیگران در سراسر جهان، ازجمله چین، مشخص کند. در اوایل اپیدمی، گروه کوچکی از ویروس‌شناسان که توسط مؤسسه ملی بهداشت آمریکا به رهبری مؤسسه ملی بهداشت گفتند که SARS-CoV-2 ممکن است از تحقیقات آزمایشگاهی ناشی شده باشد و خاطرنشان کردند که این ویروس دارای ویژگی‌های غیرعادی است که ویروس‌شناسان آمریکایی سال‌هاست در آزمایش‌ها از آن استفاده می‌کنند.

حمل‌ونقل

تحویل روباتیک مرسوله‌ها برای کاهش آلایندگی

آمازون در حال راه‌اندازی ناوگانی از دوچرخه‌های باربری الکترونیکی و تیمی از کارکنان تحویل به‌صورت پیاده برای جایگزینی هزاران ون در جاده‌های لندن است. به گزارش گاردین، این خرده فروش آنلاین نخستین هاب میکروموبایلیتی خود را در هاکنی که شرق لندن است باز می‌کند و همراه با ناوگان خودروهای برقی موجود تلاش می‌کند تا تحویل کالای ۵میلیون نفر را در سال با روشی بسیار کم آلاینده‌تر انجام دهد. این دوچرخه‌ها توسط شرکت‌های مختلف اداره می‌شوند، نه مستقیما توسط آمازون.

آمازون در سال‌جاری به‌عنوان بخشی از تلاش‌های خود برای کاهش انتشار کربن، مراکز تحویل بیشتری در سراسر بریتانیا درنظر گرفته است. این شرکت در سال ۲۰۲۰به‌عنوان مرکز حمل‌ونقل محموله با دوچرخه و پیاده در شهر لندن نام گرفت، اما این پروژه هنوز به نتیجه نرسیده است.

جان بامفری، مدیر آمازون در بریتانیا، گفت: آمازون به سمت آینده‌ای با کربن خالص صفر جهانی پیش می‌رود. یکی از راهکارهای ما، تغییر شبکه‌های حمل‌ونقل است. دوچرخه‌های باربری الکترونیکی جدید و ناوگان رو به رشد تحویل وسایل نقلیه الکتریکی ما به ما کمک می‌کنند تا در ماه‌های آینده بیش از هر زمان دیگری در سراسر لندن و بریتانیا تحویل کالا به مشتریان را بدون آلوده کردن هوا، انجام دهیم. مت کوبان، عضو کابینه شورای هاکنی برای محیط‌زیست و حمل‌ونقل، از این طرح استقبال کرد. او گفت: اگر می‌خواهیم کربن را به صفر برسانیم، مقابله با انتشار گازهای گلخانه‌ای قدم اول و مهمی است. ما واقعا خوشحالیم که با آمازون برای حمایت از خروج ون‌های سنتی از خیابان‌ها و جایگزینی آنها با دوچرخه‌های الکترونیکی همکاری کردیم. این کار به کاهش انتشار گازهای گلخانه‌ای و بهبود کیفیت هوا برای مردم در هاکنی و فراتر از آن کمک می‌کند.

طبق اعلام انجمن دوچرخه، حدود ۲۰۰۰دوچرخه باری در بریتانیا برای استفاده تجاری در سال ۲۰۲۰فروخته شد و تعداد مشابهی برای استفاده خانواده‌ها و افراد به فروش رسید. پیش‌بینی می‌شود این رقم در سال گذشته افزایش یافته باشد.

تصویرسازی: همشهری/محمدعلی حلیمی

راهکار عجیب بستن دسترسی به سامانه‌ها از خارج

برخی بانک‌ها دسترسی آی‌پی‌های خارجی را به اینترنت بانک‌های خود برای جلوگیری از حملات سایبری بسته‌اند اما این کار چقدر فایده دارد؟

امنیت

عمادالدین قاسمی‌پناه
روزنامه‌نگار

تجربه برخی از کاربران حاکی از مسدود شدن تعدادی از سامانه‌های بانکی طی چند روز گذشته است. درحالی که کسب‌وکارهای ایرانیان خارج از کشور و داخل کشور از اینترنت بانک برای انجام امور خود استفاده می‌کنند، اکنون سامانه‌های بعضی از بانک‌ها صرفا با IP ایران قابل دسترسی هستند. البته همه بانک‌ها دسترسی به سامانه‌های خود را قطع نکرده‌اند و در عین حال، آن بانک‌هایی که این کار را انجام داده‌اند نیز علت را اعلام نکرده‌اند. بانک مرکزی هم در این میان واکنشی نسبت به این اتفاق نداشته و توضیحی نداده است. با این حال، نخستین علتی که به ذهن خطور می‌کند، پیشگیری از حملات سایبری است. برخی متخصصان حوزه IT معتقدند این کار شاید چند سال پیش کارآمدی داشت، اما اکنون و با وجود روش‌های مختلف برای نفوذ به سامانه‌ها، نمی‌توان این اقدام را روشی مؤثر دانست. همچنین تعدادی دیگر از سازمان‌ها و حتی مراکز دانشگاهی هم دسترسی خارج از کشور را قطع کرده‌اند و سامانه خود را اصطلاحا از طریق عفونت بدون علامت قابل شناسایی و پیشگیری نبوده است. البته هنوز هم ممکن است که ویروس منشا طبیعی داشته باشد. نکته اصلی این است که هیچ‌کس واقعیت را نمی‌داند. به همین دلیل است که بررسی تمام اطلاعات مرتبط موجود در پایگاه‌های داده موجود در آمریکا بسیار مهم است. از زمان شروع همه‌گیری در اوایل سال ۲۰۲۰، دولت آمریکا انگشت اتهام را به سمت چین نشانه رفته است. درست است که نخستین موارد مشاهده شده کووید-۱۹ در ووهان بوده، اما داستان کامل شیوع درصورتی که به‌طور قطع روشن شود، می‌تواند نقش آمریکا را در تحقیق در مورد کرونا و به اشتراک گذاشتن بیوتکنولوژی خود با دیگران در سراسر جهان، ازجمله چین، مشخص کند. در اوایل اپیدمی، گروه کوچکی از ویروس‌شناسان که توسط مؤسسه ملی بهداشت آمریکا به رهبری مؤسسه ملی بهداشت گفتند که SARS-CoV-2 ممکن است از تحقیقات آزمایشگاهی ناشی شده باشد و خاطرنشان کردند که این ویروس دارای ویژگی‌های غیرعادی است که ویروس‌شناسان آمریکایی سال‌هاست در آزمایش‌ها از آن استفاده می‌کنند.

روش ناکارآمد

نعیم فرهادیان، متخصص شبکه در گفت‌وگو با همشهری با اشاره به اینکه اگر علت iran access کردن برخی از سایت‌ها، پیشگیری از حمله سایبری باشد، کاری بی‌فایده انجام شده، می‌گوید: «مهاجمان سایبری می‌توانند از وی‌پی‌ان‌های ایرانی برای اتصال و درنهایت نفوذ استفاده کنند.» فرهادیان در پاسخ به این پرسش که دقیقا به چه علت، مسدود کردن IP نمی‌تواند مانع حملات سایبری شود، می‌گوید: «کسی که تخصص و هدفش هک کردن یک سایت است، حتما این توانایی را هم دارد که به IP ایران دسترسی پیدا کند.»

این متخصص حوزه فناوری اطلاعات همچنین یکی از دلایلی را که برای iran access کردن عنوان می‌شود، جلوگیری از حملات DDoS می‌داند. او با اشاره به اینکه این کار در سازمان‌هایی رایج است که وقتی سامانه‌ای دچار حمله DDoS می‌شود، وب سایت را iran access می‌کنند، در توضیح این نوع حمله می‌گوید: «حملات DDoS به این معنی است که معمولا تعداد زیادی درخواست به سایت مورد نظر ارسال و به این ترتیب آن سایت از دسترس خارج می‌شود.»

زامبی‌ها همه جا هستند

به‌گفته فرهادیان «این روش ۵سال پیش، شاید می‌توانست کارایی داشته باشد، چون اکثر این نوع حملات از خارج کشور انجام می‌شد، اما اتفاقی که اکنون شاهد هستیم، این است که botnetهای ایرانی هم درست شده‌اند و در عمل مهاجم از داخل ایران هم می‌تواند حمله DDoS را انجام دهد.» این متخصص در توضیح این نوع حمله می‌گوید: «حمله محروم‌سازی از سرویس (distributed denial of service) یا همان DDoS به این مفهوم است که مهاجم به جای حمله از یک نقطه، از چند هزار نقطه به سامانه هدف حمله می‌کند.»

به‌گفته فرهادیان، «برای چنین حمله‌ای، مهاجم اصطلاحا نیاز به تعداد زیادی «زامبی» دارد و زامبی‌ها یا همان شبکه botnetها می‌توانند در خدمت مهاجم اصلی قرار بگیرند.»

او یکی از مرسوم‌ترین کارهایی را که در کشور برای جلوگیری از حملات DDoS انجام می‌شود، همین iran access کردن می‌داند، اما تأکید می‌کند که حمله DDoS صرفا از خارج از کشور صورت نمی‌گیرد.

فرهادیان با اشاره به اینکه اکنون botnetها در داخل ایران هم وجود دارند، محدود کردن دسترسی به ایران را عملی بی‌فایده می‌داند. علت این موضوع نصب بسیاری از اپلیکیشن‌های ناامن از سوی کاربران است که در ظاهر به مردم سرویس می‌دهند، اما می‌توانند در نقش یک مهاجم به یک وب سایت عمل کنند، چیزی که خارج از بحث این گفت‌وگوست. او همچنین با اشاره به انتشار مقاله‌ای در سال ۹۸که محتوای آن «حملات گسترده DDoS با سوءاستفاده از MTProxyهای تلگرام» بود، تأکید می‌کند که همین الان در داخل کشور botnet وجود دارد و iran access کردن کمکی به وب‌سایت‌ها نمی‌کند.

جلوگیری از DDoS

این کارشناس شبکه با اشاره به استفاده از راه‌حل‌های رسمی محافظت از DDoS یا DDoS protection می‌گوید: «راه‌حل‌های بسیاری برای جلوگیری از حملات DDoS وجود دارد، از تجهیزات سخت‌افزاری گرفته تا سرویس‌های ابری.»

به‌گفته فرهادیان «هنگامی که زامبی‌ها حمله می‌کنند، درواقع یک «ترافیک کثیف» ایجاد می‌کنند. اگر بتوانیم این ترافیک را از یک مرکز تصفیه ترافیک عبور دهیم، چنین مرکزی می‌تواند مانع ترافیک کثیف یا حملات DDoS شود.»

دردسر برای مردم

این متخصص فناوری اطلاعات با اشاره به اینکه اگرچه گفته می‌شود که بانک مرکزی به این بانک‌ها اعلام کرده که iran access کنند، می‌گوید: «این در حالی است که صرفا بانک‌ها از این روش استفاده نمی‌کنند و برخی از دانشگاه‌ها و سازمان‌های دولتی مانند سایت تامین اجتماعی هم به این راه‌حل روی آورده‌اند.»

فرهادیان توجه به این نکته را ضروری می‌داند که ساده‌انگارانه‌ترین روش برای بالا بردن امنیت یک سایت، همین روش است که در عمل نه‌تنها کاربردی ندارد، بلکه باعث بروز مشکل برای مردم می‌شود. به‌گفته او «این اتفاق برای بخشی از مردم چه در داخل کشور و چه خارج از کشور مشکل ایجاد می‌کند، چرا که در داخل هم از آنجا که معمولا وی‌پی‌ان‌ها فعال است، کاربران ناچار می‌شوند که برای اتصال به این سایت‌ها و سامانه‌ها وی‌پی‌ان خود را غیرفعال و دوباره فعال کنند.» این کارشناس شبکه با اشاره به اینکه تعداد وب‌سایت‌هایی که سیاست iran access را انتخاب کرده‌اند شاید چند صد وب‌سایت بیشتر نباشند، ادامه می‌دهد: «نکته قابل توجه این بود که این وب‌سایت‌ها، در شمار پرمراجعه‌ترین وب‌سایت‌ها بودند که مردم خدمات بسیاری از آنها دریافت می‌کردند.»

به‌گفته فرهادیان «فرقی نمی‌کند که ادمین این وب‌سایت‌ها از تجهیزات سخت‌افزاری استفاده کنند یا از جدیدترین تکنولوژی‌های مبتنی بر ابر، در آخر بدترین سیاست را پیاده می‌کنند.»

خطر قرص‌های مسکن برای معده و قلب

تحقیقات نشان می‌دهد که داروهای مسکن غیراستروئیدی خطر خونریزی معده و سکته‌های قلبی و مغزی را درصورت استفاده نابجا افزایش می‌دهد

پزشکی

زهرا خلجی
روزنامه‌نگار

داروهای ضدالتهابی غیراستروئیدی (NSAIDs) رایج‌ترین داروهای مورد استفاده در جهان هستند. این داروها با بستن راه تولید آنزیم سیکلواکسیژناز، باعث کاهش درد می‌شوند. به گزارش مایو کلینیک، این فرایند با جلوگیری از تولید پروستاگلاندین‌ها همچنین منجر به کاهش تورم و التهاب می‌شود. همه ما چند نوع از داروهای NSAID را بدون نسخه و با نسخه در قفسه داروهای خود داریم؛ داروهایی مانند آسپیرین، ایبوپروفن، ناپروکسن و سلکوکسیب. هنگام شروع دردهای قاعدگی و فعالیت زیاد ورزشی، ورم مفاصل یا کمردرد تشدید می‌شود و این داروها بهترین راه تسکین این دردها هستند. دکتر رابرت اچ. شمرلینگ، سال ۲۰۲۰برای بخش بهداشتی هاروارد طی گزارشی نوشت که تقریبا ۱۵درصد از جمعیت آمریکا به‌طور منظم از داروهای ضدالتهابی غیراستروئیدی با نسخه و بدون نسخه استفاده می‌کنند که این مقدار سالانه بیش از ۳۰میلیارد دوز را شامل می‌شود.

مبارزه با دردهای مزمن

در بیشتر مواقع، مصرف NSAIDها چیز خوبی است. درواقع شما دارویی مناسب برای از دست ندادن فعالیت‌های روزانه در مواقع ضروری در اختیار دارید. حتی هم‌اکنون تحقیقات بیشتری در مورد استفاده از NSAIDها در بیماران برای کمک به مبارزه با موادمخدر انجام شده است. با توجه به اینکه یک‌پنجم ما با درد مزمن زندگی می‌کنیم، مدیریت مؤثر آن یک مسئله جدی و یک حق اساسی است.

اما NSAIDها در کنار مزایایی که دارند، می‌توانند برای معده خطرناک باشند؛ حتی بیشتر از آن چیزی که تا به حال می‌دانستید. دکتر سامر آلن، پزشک خانواده در این‌باره گفت: یکی از بزرگ‌ترین نگرانی‌های ما در مورد داروهای NSAID برای بیماران احتمال خونریزی در معده، پوشش معده یا مجرای آن است. این می‌تواند به‌ویژه برای افرادی که به‌طور منظم یا طولانی‌مدت از این داروها استفاده می‌کنند، خطرناک باشد. انجمن تحقیقات روده در کانادا تخمین می‌زند که ۱۵ تا ۳۰درصد

از مصرف‌کنندگان طولانی‌مدت NSAIDها در معرض خطر ابتلا به بیماری زخم‌معده هستند که ۲تا ۴درصد از این زخم‌ها ممکن است مزمن شود.

خطرات استفاده طولانی‌مدت از مسکن‌ها

اما جایی که همه‌چیز پیچیده‌تر می‌شود، زمانی است که بیمار مجبور است یک داروی مسکن را به‌صورت وریدی به‌مدت ۱۲ساعت دریافت کند و این در حوزه گسترده تداخلات دارویی نامطلوب، بیماری‌های همزمان و تجویز بیش از حد دارو، قرار می‌گیرد. بیش از نیمی از ما اکنون به‌طور منظم یک داروی تجویزی مصرف می‌کنیم و مسئله این است که همه این داروها کنار هم خوب عمل نمی‌کنند.

مطالعه‌ای در سال ۲۰۲۱ از دانشکده پزشکی دانشگاه کریتون نشان داد که برای بیمارانی که قبلا از NSAIDها استفاده می‌کردند، افزودن داروهای مهارکننده انتخابی بازجذب سروتونین (SSRI) به‌معنای افزایش احتمال خونریزی دستگاه گوارش فوقانی تا ۷۵درصد است. حالا اگر کسی از داروهای رقیق‌کننده خون، مهارکننده‌های ACE، مسدودکننده‌های بتا یا سایر NSAIDها استفاده کند، چه می‌شود؟ همه این ترکیبات می‌توانند باعث تحریک معده یا سایر عوارض جانبی شوند. برای بیمار مبتلا به التهاب روده چه اتفاقی می‌افتد؟ NSAIDها می‌توانند علائم او را بدتر کنند. بیش از یک‌دهه پیش، تحقیقات در مجله انجمن مدیران پزشکی آمریکا هشدار داد که استفاده طولانی‌مدت از داروهای ضدالتهابی غیراستروئیدی خطر ابتلا به زخم معده، نارسایی حاد کلیه و سکته مغزی و سکته قلبی را در سالمندان افزایش می‌دهد.

دوراهی تسکین درد و خونریزی معده

اما حتی برای افرادی که کاملا سالم هستند، ملاحظات مهمی وجود دارد که قبل از مصرف NSAID ها باید درنظر گرفته شود. گزارشی در سال ۲۰۱۶در مجله British Journal of General Practice هشدار داد: از نخستین روز استفاده از مسکن‌های غیراستروئیدی، شما در معرض خطر خونریزی گوارشی، سکته قلبی و سکته مغزی هستید. تحقیقاتی که ماه گذشته در کانادا منتشر شد، نشان می‌دهد که مصرف داروهایی مانند ایبوپروفن و استروئیدها برای تسکین دردهای کوتاه‌مدت می‌تواند شانس ابتلا به درد مزمن را افزایش دهد.

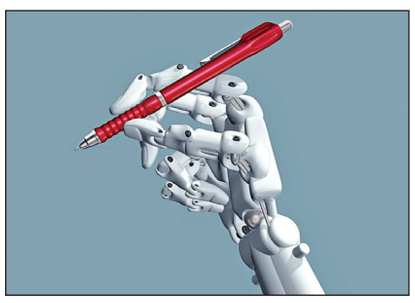
مصرف با نظر پزشک

بنابراین برای پایان دادن به چرخه قرص خوردن و معده‌درد چه کاری می‌توان انجام داد؟ اول از همه، خطرات و مزایای آن را باید درنظر گرفت. قبل از مصرف هر دارویی حتی داروهایی بدون نسخه با پزشک خود مشورت کنید. در زمان درد، دوز داروها را به‌طور خودسر بالا نبرید و به اندازه تجویز شده مصرف کنید. یک مطالعه در سال ۲۰۱۸در دانشگاه بوستون نشان داد حدود ۱۵درصد از بزرگسالانی که ایبوپروفن یا سایر NSAIDها را مصرف می‌کنند از حداکثر دوز توصیه شده روزانه برای این داروها فراتر رفته‌اند و این کار خطر عوارض جانبی جدی مانند خونریزی داخلی و حملات قلبی را افزایش می‌دهد. نکته مهم دیگر این است که NSAIDها را باید همراه با غذا مصرف کنید. اما بهتر این است که برای هر دردی داروی مخصوص تجویز شود؛ به‌عنوان مثال اگر فردی سردرد سینوسی دارد، ممکن است بهترین کار تجویز آنتی‌بیوتیک برای عفونت یا آنتی‌هیستامین برای کاهش تورم باشد؛ نه NSAIDها. برای برخی از افراد، ممکن است مصرف یک مهارکننده پمپ پروتون مانند پریلوسک (امپرازول) نیز مناسب باشد تا به محافظت از پوشش معده در برابر آسیب کمک کند.

فناوری

مقاله علمی الگوریتم هوش مصنوعی درباره خودش

الگوریتم هوش مصنوعی GPT-3 برای نخستین بار یک مقاله آکادمیک درباره خودش نوشته و این مقاله اکنون در مرحله داوری برای انتشار در نشریه‌ای علمی قرار دارد.



محقق سوئدی، «المیرا عثمانوویچ تونستروم» در مقاله‌ای در وب‌سایت Scientific American می‌گوید: این پروژه ابتدا به‌عنوان یک آزمایش ساده آغاز شد تا مشخص شود که الگوریتم تولید متن OpenAI با چه کیفیتی می‌تواند درباره خودش بنویسد. اما حالا نتیجه کار در یک مجله علمی در دست داوری قرار دارد. دستور اولیه‌ای که تونستروم به این الگوریتم داد بسیار ساده بود: «یک مقاله ۵۰۰کلمه‌ای درباره GPT-3 بنویس و ارجاعات و منابع علمی را به متن اضافه کن.» الگوریتم GPT-3 در نهایت در عرض ۲ ساعت مقاله‌ای نوشت که عنوان آن چنین است: «آیا GPT-3 می‌تواند به‌خودی خود و با کمترین دخالت انسانی یک مقاله آکادمیک بنویسد؟» این مقاله هم اکنون به‌صورت پیش‌چاپ در مرجع HAL منتشر شده است.

اینترنت

جنجال هک شدن حساب‌های کاربری ارتش انگلیس

حساب‌های شبکه‌های توییتر و یوتیوب ارتش بریتانیا بعد از مدتی هک‌شدن، دوباره بازیابی شدند.

به گزارش رویترز، حساب‌های شبکه‌های اجتماعی توییتر و یوتیوب ارتش انگلیس بعد از مدتی هک شدن، بازیابی شده‌اند. در حساب‌های ارتش بریتانیا که در این مدت هک شده بود مطالب مرتبط به رمزارزها و توکن‌های غیرمثلی (NFT) پست می‌شد.

ارتش بریتانیا در توییتی گفت: «بابت قطع موقت مطالب‌مان پوزش می‌خواهیم. ما تحقیقات کاملی را انجام خواهیم داد و از این اتفاق خواهیم آموخت.»

حساب یوتیوب ارتش هم که به آرک اینوست «Ark Invest» تغییر نام داده شده بود و چندین ویدئو مربوط به رمزارزها را پخش کرده بود، به حالت اولیه خود بازگردانده شده است. حالا حساب توییتر ارتش هم‌اکنون ۳۶۲ هزار دنبال‌کننده دارد و دنبال‌کنندگان کانال یوتیوب ارتش هم به ۱۷۷ هزار مشترک رسیده است.

آرک اینوست نام یک شرکت سرمایه‌گذاری آمریکایی با محدوده فعالیت جهانی است که در سال ۲۰۱۴ تاسیس شده بود.

عدد خبر

۱ میلیارد

یک هکر یا گروهی از هکرهای ناشناس ادعا کرده‌اند که پس از حمله به پایگاه داده پلیس شانگهای، اطلاعات بیش از یک میلیارد شهروند چین را سرقت کرده‌اند. کارشناسان از این حمله سایبری به‌عنوان بزرگ‌ترین نقض امنیت سایبری در تاریخ این کشور یاد کرده‌اند.

میزان اطلاعات سرقت شده بیش از ۲۳ترابایت است و شامل نام، آدرس، محل تولد، شماره ملی، شماره تلفن و اطلاعات پرونده جنایی شهروندان می‌شود. هکر ناشناس قصد دارد تا این داده‌ها را به قیمت ۱۰بیت کوین (حدود ۲۰۰هزار دلار) به فروش برساند.

۱۲ ماه

فروش NFT (توکن‌های غیرقابل تعویض) تحت‌تأثیر ریزش رمزارزها قرار گرفته‌اند و درآمد این بازار به پایین‌ترین سطح خود در ۱۲ماه گذشته رسیده است. نشریه گاردین براساس داده‌های شرکت تحقیقاتی حوزه کریپتو Chainalysis در گزارش خود توضیح می‌دهد که مجموع فروش NFT در ماه ژوئن به کمی بیشتر از یک میلیارد دلار رسیده که در طول یک سال گذشته، بدترین عملکرد آن بوده است.