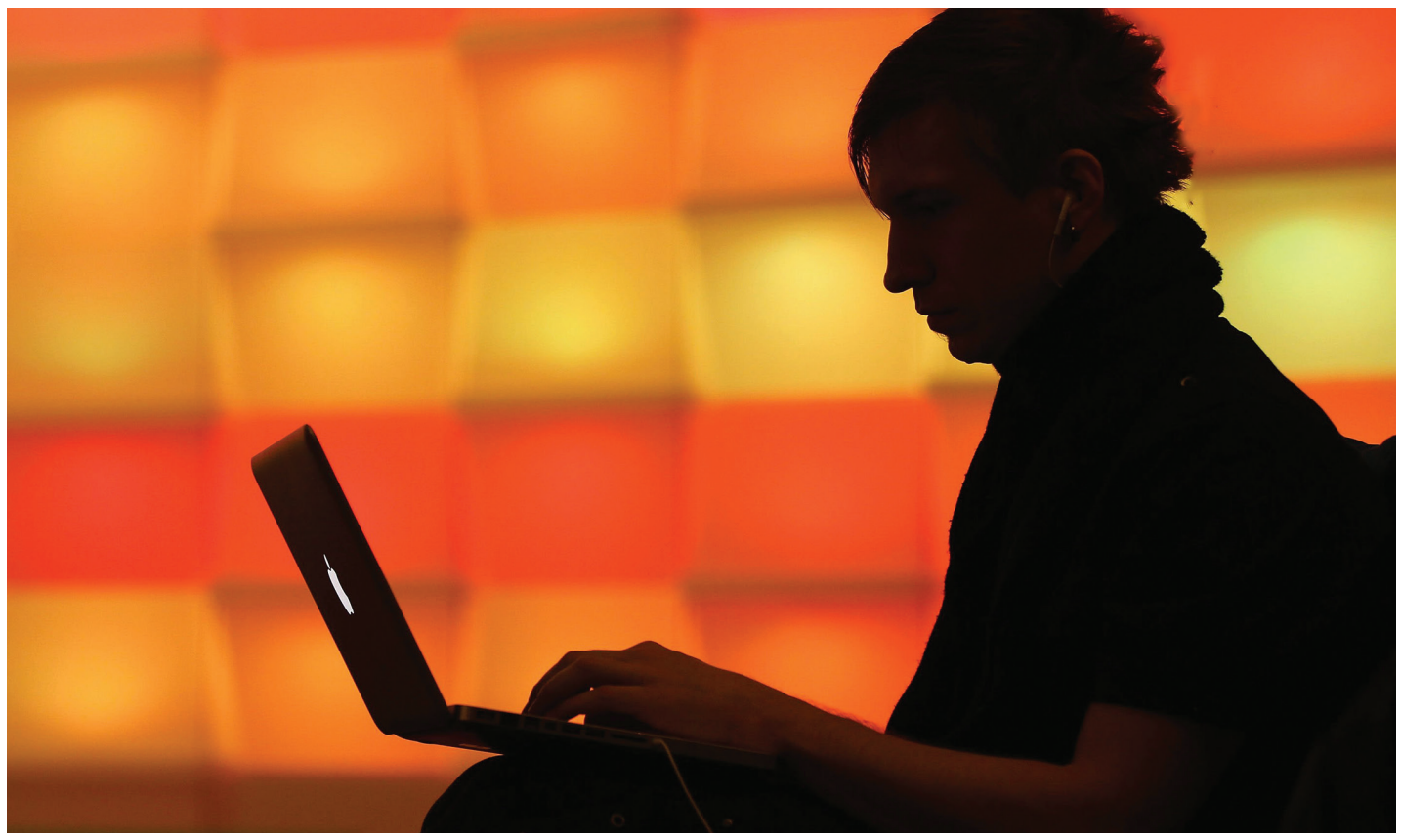
فرهیختگان
@farhikhtegandaily
WWW.FDN.IR

گزارش «فرهیختگان» از چالش سرقت اطلاعات در دانشگاه‌ها علاوه‌بر بحران کرونا و وضعیت وخیم مالی

رشد حملات سایبری به دانشگاه‌های جهان

ندا اظهری
مترجم

به‌نظر می‌رسد کووید-۱۹ تنها ویروسی نیست که دانشگاه‌ها باید نگران آن باشند و ویروس‌های دیگری چون بدافزارها و حملات سایبری هم مانند ویروس به‌جان امنیت یک کشور و یک مرکز می‌افتند. داده‌ها و اطلاعات افراد و گاه محرمانه، منابعی هستند که معمولا در معرض خطر حمله‌های سایبری و اینترنتی قرار دارند و بعضی مواقع لطمه‌های زیادی به بدنه یک کشور وارد می‌کنند. با رشد فعالیت‌های اینترنتی و آنلاین شدن کارها و ذخیره اطلاعات در فضای سایبری در دنیا، شاهد افزایش روزافزون این سوءاستفاده‌های اینترنتی و دزدیده شدن اطلاعات هستیم که گاه فضای ناامنی را برای رد و بدل کردن اطلاعات فراهم می‌آورد. در ماه‌های اخیر که بسیاری از دانشگاه‌های جهان با بحران کرونا دست‌وپنجه نرم می‌کردند، بحران دیگری با عنوان حمله‌های سایبری هم مزید بر علت شده و هزینه‌های گزافی را روی دست دانشگاه‌ها و سیستم آموزش عالی کشورها گذاشته‌اند.



رشد ۸ درصدی حمله بدافزاری

هفته گذشته، مرکز ملی امنیت سایبری انگلیس به دانشگاه‌ها و بخش آموزش عالی نسبت به افزایش حملات بدافزارها و حملات سایبری هشدار داد. برخی آزادسازی‌های اطلاعاتی که به‌دنبال شیوع ویروس کرونا رخ داده، دست‌کم یک‌سوم دانشگاه‌های انگلیس را در معرض خطر حمله بدافزارها قرار داده است. اما این خطر تنها دانشگاه‌های انگلیس را تهدید نمی‌کند. در ماه ژوئن بود که دانشگاه کالیفرنیا، سانفرانسیسکو، حدود ۱/۱۴ میلیون دلار برای دستیابی به داده‌ها پرداخت کرد. مساله حملات سایبری این روزها تبدیل به پدیده‌ای جهانی شده است به‌طوری که گروه مشاوره CyberEdge برآورد کرده است که حدود ۶۲ درصد سازمان‌های جهان در سال ۲۰۲۰ با نوعی حمله بدافزاری روبه‌رو می‌شوند؛ این درحالی است که آمارهای سال گذشته حکایت از درگیری ۵۶ درصدی با بدافزارها دارد و در مقایسه با سال گذشته، این حملات سایبری ۸ درصد رشد داشته است.

به گزارش تایم، کارشناسان این حوزه بر این باورند که قرنطینه ماه‌های اخیر به‌دلیل همه‌گیری ویروس کرونا شرایط را برای هکرها مساعدتر کرد تا آنها بتوانند از نقاط ضعف موجود در انتقال سریع کارها از راه دور و خطاهایی که در سیستم‌های آنلاین وجود دارد، نهایت استفاده را کرده و نسبت به سرقت اطلاعات اقدام کنند. مهم‌ترین بخش این مشکل و سوءاستفاده‌هایی که هکرها در سرقت اطلاعات از سیستم‌های اینترنتی می‌کنند، به‌استفاده از سیستم‌های شخصی برمی‌گردد که معمولا نرم‌افزارهای متصلی نداشته و کنترل ویروس به‌خوبی روی آنها صورت نگرفته و اتصالات وای‌فای آن کدگذاری شده نیست. با وجود این، اغلب این خطاها بیشتر از آنکه فنی باشند، خطاهای انسانی هستند که هکرها غالبا با دستیابی به رمز عبور کاربران سعی می‌کنند حمله خود را انجام دهند. بسیاری از ویروس‌ها در قالب ایمیل برای کاربران ارسال می‌شود و هکرها سعی می‌کنند عناوین خاصی را مانند کووید برای ایمیل انتخاب کنند تا کاربران وسوسه شوند و آن را باز کنند. با باز شدن ایمیل، حمله سایبری آغاز می‌شود و بدافزار روی سیستم کامپیوتر کاربر نصب شده و اقدام به سرقت اطلاعات می‌کند. دانشگاه‌ها برای جلوگیری از بروز حملات سایبری تا جایی که توانسته‌اند از فرآیند احراز هویت چند عاملی و از فایروال‌های به‌روزرسانی شده استفاده و تلاش کرده‌اند از اطلاعات خود بک‌آپ تهیه کنند. اما این کار برای برخی مراکز آموزشی و دانشگاه‌ها دیر شده و هکرها اطلاعات مورد نظر خود را از سیستم‌های ناامن اطلاعاتی آنها به سرقت برده‌اند. هکرها در قبال پرداخت هزینه‌های سنگین حاضر به برگرداندن اطلاعات هستند.

دوراهی دشوار پیش‌روی دانشگاه‌ها

این قبیل حملات سایبری می‌توانند یک سازمان را با اطلاعات مهمی که دارد، فلج کند چراکه نگرانی از قطع طولانی‌مدت کسب‌وکار و آسیبی که از نظر اعتبار به پایه‌های آن وارد می‌شود، هرگز قابل جبران نیست به‌طوری که تمام مسئولیت حفاظت از اطلاعات به سرقت رفته بر عهده آن سازمان بوده و موظف است برای حفاظت از این داده‌ها هم که شده، هزینه‌های گزافی را بپردازد. اما مساله‌ای که در اینجا مطرح می‌شود این است که در شرایط کرونایی که بسیاری از دانشگاه‌ها با بحران‌های مالی و کاهش بودجه‌ها روبه‌رو هستند، مواجهه با حملات سایبری و سرقت اطلاعات، آنها را بر سر دوراهی پرداخت یا عدم‌پرداخت مبالغ درخواستی از سوی هکرها قرار می‌گیرند. در این میان، مرکز ملی امنیت سایبری انگلیس به دانشگاه‌ها توصیه می‌کند که چنانچه با حمله سایبری و درخواست پرداخت مبالغ گزاف برای برگرداندن اطلاعات به سرقت رفته مواجه شدند، پولی را به هکرها نپردازند. این مرکز دلایلی را هم برای این ادعا بیان کرده است اما اصلی‌ترین آنها این است که مسئولان دانشگاه نمی‌توانند اطمینان حاصل کنند که هکر، آسیب وارد آمده را اصلاح کرده و تصمیم نداشته باشد بار دیگر از اطلاعات هک شده سوءاستفاده کند. معمولا کسانی که تسلیم هکرها شده و راضی به پرداخت مبالغ خواسته شده می‌شوند، حساسیت فعالیت‌ها و مصلحت کار را دلیل آن عنوان می‌کنند. بعضی دیگر هم به گفته هکرها اعتماد می‌کنند و به این امید مبلغ درخواستی را پرداخت می‌کنند که هکر به تعهدش وفادار بماند.

امنیت سایبری در اولویت

سال‌هاست بحث امنیت سایبری در دنیا مطرح می‌شود و درحال حاضر با توجه به رشد چند برابری حملاتی که رخ می‌دهد، فراتر از نرم‌افزارهای آنتی‌ویروس و سیستم‌های دفاعی فنی رفته است. برخی شرکت‌های متخصص در حوزه امنیت سایبری اقدام به استخدام کارشناسانی می‌کنند که بتوانند مشتریان خود را مجاب کنند که آیا باید به هکرها اعتماد کرد؟ البته در این میان، ارزیابی خطر پرداخت مبلغی که هکر در قبال برگرداندن اطلاعات درخواست کرده، به انگیزه هکر به سرقت اطلاعات بستگی دارد. جورج کرتز، مدیر اجرایی شرکت امنیت سایبری CrowdStrike می‌گوید: «در حالی که اقدام مجرمان قابل پیش‌بینی است و با وجود اینکه می‌دانیم ساده‌ترین و بی‌دردسرترین راه را برای سرقت اطلاعات استفاده می‌کنند، اما فعالیت‌های دولت‌ها اغلب بی‌وقفه‌تر و پیچیده‌تر است و درنتیجه کار برای مدافعان سیستم‌ها و فضاهای سایبری هم چالش برانگیزتر می‌شود.»

اما سوالی که در اینجا مطرح می‌شود، این است که چرا هکرها دانشگاه‌ها را مورد هدف حمله‌های سایبری خود قرار می‌دهند؟ هکرها به‌دنبال دستیابی به مالکیت معنوی در تحقیقات پیشرفته هستند و به‌ویژه با شیوع ویروس کرونا، عطش آنها به دستیابی به منبع اصلی تحقیقاتی کرونایی بیشتر شده است. با توجه به اینکه دنیا برای هر بخش از ابعاد زندگی بیش از هر زمان دیگری وابسته به فناوری‌های روز شده، دانشگاه‌ها باید بیش از پیش به توصیه مرکز ملی امنیت سایبری توجه کرده و آگاهی خود را درباره موضوعات مرتبط با امنیت سایبری در جوامع بالا برده و در مقاوم‌سازی سیستم‌های اطلاعات سرمایه‌گذاری کنند. همان‌طور که دانشگاه‌ها برای بهبود پشتیبانی خود از آموزش از راه دور و آنلاین در حال تغییر استراتژی‌های دیجیتالی خود هستند، باید انعطاف‌پذیری خود را هم در برابر حمله‌های سایبری درنظر بگیرند تا درصورت گرفتار شدن در دام هکرها بتوانند در موقع لازم، واکنش مناسب را نشان دهند. کارشناسان توصیه می‌کنند دانشگاه‌ها بیشتر باید روی امور دفاعی سرمایه‌گذاری کنند تا مجبور نشوند برای بازگرداندن اطلاعات هک شده، هزینه‌های سنگینی را به هکرها بپردازند.

تشکیل گروه‌های امنیت سایبری

همان‌طور که گفتیم، درحال‌حاضر حملات سایبری تنها محدود به کشوری خاص نمی‌شود و تقریبا هیچ کشوری از این حمله‌ها در امان نیست. در ماه‌های اخیر، هلند، آلمان و بلژیک هم جزء کشورهایی بوده‌اند که به‌ویژه دانشگاه‌هایشان مورد حمله هکرها و اطلاعات آنها درمعرض خطر قرار گرفته‌اند. به‌گفته معاون رئیس دانشگاه هلند، یکی از موثرترین شیوه‌های پیشنهادی برای خلاصی از شر هکرها این است که دانشگاه‌ها برای حفاظت از خود دربرابر تلاش‌های پیچیده هکرها به‌منظور دستیابی به اطلاعات باید گروه‌های مشترک امنیت سایبری تشکیل دهند. دانشگاه هلند یکی از همین قربانیان است که درحوالی کریسمس مورد حمله سایبری هکرها قرار گرفت و برای بازگرداندن اطلاعات به‌سرقت رفته مجبور به پرداخت ۱۷۵ هزار یورو به مجرمان شد. نیک باس از دانشگاه ماستریخت معتقد است که یکی از درس‌های حمله سایبری برای دانشگاه‌ها این است که آنها نباید به سیستم‌های امنیتی خود اعتماد کامل داشته باشند. کریسمس سال گذشته بود که هکرها کنترل سرورهای ارسال ایمیل و ذخیره نتایج اطلاعات دانشگاه را تحت‌کنترل خود درآوردند. بازیابی کلی سیستم بیش از یک ماه زمان برد و دانشگاه مجبور شد برای به‌دست آوردن دوباره اطلاعات ۳۰ بیت‌کوین به‌مهاجمان بپردازد.

دکتر باس با بررسی خطای رخ داده و چگونگی توقف این حملات در آینده، به دانشگاه‌ها توصیه می‌کند که سیستم‌های امنیتی خود را یکپارچه کنند. او در این گزارش به سیستم امنیت سایبری یکپارچه و همکاری دانشگاه‌های آمریکا و کانادا اشاره کرد. این مساله فقط به این برنمی‌گردد که آیا دانشگاه‌ها از پس هزینه‌های حملات سایبری برمی‌آیند یا نه. درواقع، وقتی صحبت از برقراری امنیت سایبری می‌شود، گزینه دیگری وجود ندارد جز اینکه دانشگاه‌ها باید سرمایه‌گذاری بیشتری روی این بخش داشته باشند. از زمان حمله هکرها به دانشگاه‌های هلند، این مراکز آموزشی تلاش‌های خود را برای همکاری‌های مشترک افزایش داده‌اند تا بتوانند به‌طور شبانه‌روزی امنیت شبکه‌های فناوری اطلاعات خود را برقرار کنند. از آنجا که دانشگاه‌ها میزبان هزاران دانشجویی هستند که از لپ‌تاپ‌های شخصی استفاده می‌کنند و محققان هم اطلاعات را به‌طور آزاد به اشتراک می‌گذارند، در صدر هدف نرم هکرها برای اجرای حملات سایبری قرار دارند. سرقت اطلاعات در دانشگاه ماستریخت، تنها یک نمونه از چند حمله سایبری است که طی ماه‌های اخیر در دانشگاه‌های اروپا صورت گرفته است. دسامبر سال گذشته، هزاران دانشجو در دانشگاه «گیسن» آلمان به‌دنبال یک حمله سایبری مجبور شدند رمز عبور جدیدی را به‌طور دستی برای ورود به سیستم دریافت کنند. در ماه اکتبر هم ایمیل و سیستم اطلاعات دانشجویان دانشگاه «آنتورپ» بلژیک در اقدامی جداگانه مورد حمله سایبری هکرها قرار گرفت. به‌طورکلی، دانشگاه‌ها و موسسه‌های آموزش عالی آمریکا ۳/۶ درصد از کل بودجه فناوری اطلاعات را صرف برقراری امنیت اطلاعات می‌کنند که به‌نظر می‌رسد پایین‌ترین سطح هزینه‌ای است. اما از سوی دیگر، مطالعاتی که ازسوی افسران ارشد اطلاعاتی صورت گرفته حاکی است شرکت گروه بین‌المللی داده‌ها وابسته به دانشگاه ماساچوست به‌طور متوسط ۱۶ درصد از بودجه اختصاص داده شده به بخش فناوری اطلاعات را صرف امنیت سایبری خود می‌کند.

دانشگاه‌های ایندیانا، نورث وسترن، پوردو، راتگرز و نبراسکا در سال ۲۰۱۸ در جلسه‌ای که داشتند با راه‌اندازی یک مرکز مشترک امنیت سایبری موسوم به OmniSOC تلاش کردند با همکاری یکدیگر امنیت سایبری دانشگاه‌های خود را برقرار و از اطلاعات دانشجویان خود محافظت کنند. به گفته آنها، سیستم‌های دانشگاه‌ها به‌طور واحد برای دفاع دربرابر حملات سایبری کافی نیست و هکرها با اقداماتی پیچیده به‌راحتی می‌توانند به آن نفوذ کنند. اما چنین مرکزی می‌تواند تمام شبکه‌های دانشگاهی را به‌طور همزمان نسبت به فعالیت‌های مشکوک سایبری کنترل کند و درصورت مشاهده اقدامی مشکوک، سریع واکنش نشان دهد. ۶ دانشگاه کانادایی شامل دانشگاه‌های مک گیل، مک‌مستر، ریرسون، آلبرتا، بریتیش کلمبیا و تورنتو با مشارکت هم در سال ۲۰۱۸ اقدام به تشکیل مرکز مشترک امنیتی به نام CanSSOC کردند تا بتوانند با سرعت بیشتری، تهدیدهای غیرمنتظره هکرهای اینترنتی را پاسخ دهند.

چارسوی فناوری

بزرگ‌ترین تراشه‌ساز چینی جدیدترین هدف تحریم‌های آمریکا

به گزارش مهر به نقل از رویترز، ایالات‌متحده آمریکا محدودیت‌های جدیدی بر صادرات به SMIC، بزرگ‌ترین تراشه‌ساز چینی وضع کرده است. دولت آمریکا ادعا می‌کند ریسک آن وجود دارد که تجهیزاتی که برای این شرکت تامین می‌شود برای مقاصد نظامی به کار رود. طبق نامه وزارت بازرگانی آمریکا، تامین کنندگان برخی تجهیزات SMIC اکنون باید هرکدام به‌طور جداگانه مجوز صادرات دریافت کنند. این اقدام نشان‌دهنده تغییر سیاست آمریکا نسبت به اوایل سال جاری میلادی است. به گفته سه منبع آگاه از امر، در اوایل سال جاری وزارت بازرگانی به متقاضیان مجوز «کاربر نهایی نظامی» برای فروش تجهیزات به SMIC اعلام کرده بود نیازی به چنین اجازه‌نامه‌ای نیست. تراشه‌ساز چینی اعلام کرده هیچ هشدار رسمی درباره اعمال محدودیت‌ها دریافت نکرده و علاوه‌بر آن هیچ ارتباطی با ارتش چین ندارد. این شرکت در بیانیه‌ای اعلام کرد: «SMIC تاکید می‌کند که نیمه‌رسانا تولید کرده و فقط برای مصارف تجاری و مدنی سرویس فراهم می‌کند. این شرکت هیچ رابطه‌ای با ارتش چین ندارد و برای هیچ کاربر نظامی محصول تولید نمی‌کند.»

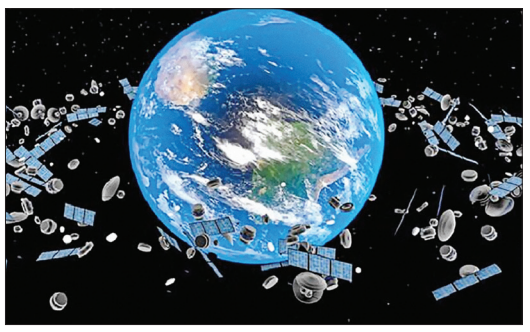
SMIC جدیدترین شرکت برتر چین در حوزه فناوری است که با محدودیت‌های تجاری از سوی آمریکا روبه‌رو می‌شود.

کرونا اقبال به تبلت‌های دارای نمایشگرهای بزرگ را افزایش داد

به گزارش مهر به نقل از زددی‌نت، رشد سرعت فروش تبلت‌ها از سال ۲۰۱۴ تا امروز بی‌سابقه بوده و عامل این مساله شیوع کرونا و خانه‌نشینی میلیون‌ها کارمند، دانش‌آموز، دانشجو و... در سراسر جهان بوده که مجبور شده‌اند برای انجام فعالیت‌های شخصی و حرفه‌ای از تبلت استفاده کنند. بررسی‌های موسسه استراتژی آنالیتیکس نشان می‌دهد با عرضه گوشی‌های هوشمند همه کاره و دارای نمایشگرهای نسبتا بزرگ، رونق بازار تبلت در ابتدای دهه جاری میلادی به پایان رسیده است اما شیوع ویروس کرونا این شرایط را تغییر داد و باعث شد خرید تبلت به‌خصوص برای استفاده‌های آموزشی و حرفه‌ای بیشتر شود. برهمین اساس فروش تبلت در سال ۲۰۲۰ نسبت به سال ۲۰۱۹ حدود یک درصد افزایش یافته، این درحالی است که از سال ۲۰۱۴ تا ۲۰۱۹ به‌طور مرتب رشد منفی برای فروش تبلت ثبت شده است. ازجمله پرطرفدارترین تبلت‌های عرضه‌شده در بازار آی‌پد پروی اپل و نیز سرفیس پروی مایکروسافت است. عرضه برخی از این تبلت‌ها همراه با صفحه کلید موجب بیشتر شدن محبوبیت آنها شده است. براساس پیش‌بینی استراتژی آنالیتیکس دوسوم میزان فروش بازار تبلت تا سال ۲۰۲۵ مربوط به تبلت‌هایی خواهد بود که نمایشگرهای ۱۰ اینچی و بزرگ‌تر دارند.

ابزاری برای تشخیص سریع و کم‌هزینه کروناویروس

به گزارش ایسنا و به نقل از فیز، پژوهشگران دانشگاه وارویک (University of Warwick) انگلستان در بررسی جدیدی نشان داده‌اند که یک ابزار تشخیصی جدید می‌تواند با بررسی ترکیبات قندی بدن، به شناسایی کووید-۱۹ بپردازد. ابداع این ابزار، گام قابل توجهی در تشخیص کووید-۱۹ به‌شمار می‌رود و امکان آزمایش قابل اطمینان را در آینده فراهم می‌کند. تشخیص کووید-۱۹ درحال‌حاضر به تجهیزات گوناگون و ابزاری مانند سواب بینی نیاز دارد و آماده شدن نتایج آزمایش‌ها نیز زمان می‌برد. شاید ابزاری که پژوهشگران دانشگاه وارویک ابداع کرده‌اند، بتواند امکان تشخیص عفونت ناشی از کروناویروس را بدون نیاز به تجهیزات متداول فراهم کند. این ابزار تشخیصی، از قندهای موسوم به گلیکان (glycan)، برای شناسایی ویروس استفاده می‌کند. کاربرد آن به ابزار خانگی بررسی بارداری شباهت دارد. در شرایط کنونی همه‌گیری کروناویروس، نیاز فوری به ابزار تشخیصی جدید به‌خصوص ابزاری که نتایج آزمایش را به‌سرعت آماده می‌کنند، احساس می‌شود. پروفسور متیو گیبسون (Matthew Gibson)، از پژوهشگران این پروژه گفت: «گروه ما، کارآیی این روش تشخیصی را با آزمایش آن روی یک ویروس مشابه کروناویروس که جایگزین ایمن‌تری برای بررسی است، نشان داده‌اند.



هویت نامعلوم ۷۵ درصد آشغال‌های فضایی در مدار زمین

به گزارش مهر به نقل از نیواطلس، پژوهشی که برای شناسایی هویت آشغال‌های فضایی که در مدار ۳۶ هزار کیلومتری زمین حرکت می‌کنند، انجام شده، نشان می‌دهد هویت و ماهیت ۷۵ درصد از آنها غیرقابل تشخیص است. این زباله‌های فضایی عملکرد ماهواره‌های ناوبری، مخابراتی و بررسی آب‌وهوا را مختل می‌کنند. برخی از این زباله‌های فضایی تا بدان حد کوچک هستند که کنترل و شناسایی آنها کار ساده‌ای نیست. حدس زده می‌شود بخش اعظم این زباله‌ها همان بخش‌های قدیمی و از کارافتاده ماهواره‌ها باشند، اما با گذشت مدت زمان طولانی دیگر نمی‌شود ماهیت دقیق بسیاری از آنها را تشخیص داد. محققان هشدار می‌دهند برخورد و تصادف برخی از این زباله‌ها با یکدیگر می‌تواند آلودگی مدار زمین را بیشتر کند. ازجمله در فوریه سال ۲۰۰۹ برخورد دو ماهواره از رده خارج‌شده باعث خرد شدن آنها و پراکنده شدن صدها قطعه کوچک این دو ماهواره در فضا شد. بررسی ناسا که با همکاری محققان انگلیسی، یک نرم‌افزار ویژه و تلسکوپ ۲/۵۴ متری اسحاق نیوتون در مراکش انجام شده، نشان می‌دهد ۹۵ درصد از قطعات زباله‌های فضایی حدود یک متر یا کمتر طول دارند و لذا شناسایی، تعقیب و مقابله با خطرات با آنها کار دشواری است.