مشخصات احتمالی گوشی آنر X۱۰ پرو فاش شد

به تازگی یکی از گوشی‌های هوشمند مرموز آنر در سایت TENAA مشاهده شده است.

به گزارش باشگاه خبرنگاران جوان، ما تاکنون شایعاتی درباره گوشی‌های آینده آنر شنیده‌ایم، حتی به ما گفته شده است که این دو دستگاه X۱۰ مکس و X۱۰ پرو نام خواهند داشت. در حالی که X۱۰ مکس دارای صفحه نمایش بزرگی با قطر بیش از ۷ اینچ است، گفته می‌شود که X۱۰ Pro دارای ابعادی "معمولی" است که در جایی بالاتر از آستانه ۶ اینچ قرار دارد.

یک گوشی دیگر با لنز پریسکوپی

به تازگی گوشی هوشمندی با شماره مدل‌های BMH-TN۲۰ و BMH-AN۲۰ با مشخصات و عکس‌های کامل در TENAA ظاهر شده است و نشان می‌دهد که برند هوآوی قصد دارد گوشی دیگری با لنز پریسکوپی به بازار عرضه کند.

مشخصات گوشی مرموز آنر

سی‌پی‌یو این دستگاه با عنوان ۲.۵۸ گیگاهرتزی ذکر شده است، که میزان هسته بزرگ Cortex-A۷۶ در تراشه Kirin را نشان می‌دهد. این دستگاه با پیکربندی‌های رم ۶ گیگابایتی و ۸ گیگابایتی در این فهرست دیده می‌شود، در حالی که حافظه ذخیره‌سازی آن گزینه ۲۵۶/۱۲۸ گیگابایت است. از نظر دوربین، انتظار داریم در این گوشی یک دوربین چهارگانه ببینیم که لنز اصلی آن ۴۰ مگاپیکسلی است، اما یک شوتر پریسکوپی نیز در عکس‌ها وجود دارد. برخی ممکن است نکات بسیار متفاوتی را بین BMH-TN۲۰ و Honor ۳۰ مشاهده کنند که دارای شماره مدل BMH-TN۱۰ است. با این حال، منابع چینی ادعا می‌کنند که این تلفن هوشمند کاملاً جدید است.

باید برای کسب اطلاعات دیگر از گوشی مرموز آنر کمی بیشتر منتظر ماند زیرا مطمئنا در آینده، شرکت سازنده آن جزئیات بیشتری از مشخصات آن را در اختیار کاربران قرار می‌دهد.

البته گاهی مواقع گوشی‌های هوشمند بدون هیچ اطلاع قبلی عرضه می‌شوند و همین مسئله باعث می‌شود اطلاعات کمتری از آن‌ها در فضای مجازی درز پیدا کند. باید دید که آنر از کدام استراتژی برای محصول جدیدش استفاده می‌کند.

پدیده عجیبی که روی سیاره مریخ مشاهده شد!

محققان با کمک داده های مدارگرد فضایی اروپا موفق به مشاهده پدیده‌ای جالب روی سیاره سرخ شده اند.

به گزارش سباشگاه خبرنگاران جوان، مرّیخ یا بَهرام که به انگلیسی مارس گفته می‌شود چهارمین سیاره در منظومه شمسی است. این سیاره همچنین با نام سیاره سرخ نیز شناخته می‌شود. در نمونه گیری و آزمایشی که از خاک سطح مریخ انجام شده بود نشان می‌داد که سطح مریخ بافتی بازالتی دارد که نوعی سنگ آتش‌فشانی، مشابه شن‌های سواحل هاوایی است.

اما به تازگی ثبت پدیده ای جالب روی این سیاره سرخ خبرساز شده است. محققان با استفاده از طیف‌سنج مرئی و ماوراء بنفش «NOMA» موجود در مدارگرد ردیاب گاز اگزومارس یک لایه درخشان از نور سبز را در اطراف این سیاره مشاهده کرده اند.

طبق پژوهشی که روز دوشنبه در مجله «Nature Astronomy» منتشر شد مدارگرد ردیاب گاز آژانس فضایی اروپا، اکسیژنی را ردیابی کرده که موجب ایجاد لایه نور سبز در جو مریخ می‌شود. این اولین بار است که چنین رنگ سبزی در سیاره‌ای دیگر به غیر از زمین مشاهده می‌شود. مشاهده این پدیده در اطراف مریخ نتیجه رصد ۴۰ ساله برای پدیده‌های موجود در سیاره سرخ است.

گفتنی است؛ «مدارگرد ردیاب گاز اگزومارس» که در اکتبر سال ۲۰۱۶ میلادی به مریخ رسید قرارگرفتن آن در مدار صحیح این سیاره بیش از یک سال به طول انجامید. این مدارگرد از ماه مه سال ۲۰۱۸ میلادی شروع به اندازه‌گیری‌های مختلف در سیاره سرخ کرد.

اضافه شدن قابلیت پخش شبکه‌های تلویزیونی به پیام رسان سروش

پیام رسان سروش به تازگی امکان دسترسی به شبکه‌های تلویزیونی داخلی و برون مرزی را برای کاربران خود فراهم کرده است.

به گزارش باشگاه خبرنگاران جوان، اخیرا پیام رسان سروش قابلیتی را اضافه کرده است که به کاربران امکان پخش زنده شبکه‌های تلویزیونی داخلی شبکه‌های ایرانی برون مرزی و رادیویی را می‌دهد.

این قابلیت در بخش ویترین سروش قرار گرفته است و کاربران از این طریق می‌توانند به صورت زنده به شبکه‌های تلویزیونی دسترسی داشته باشند. علاوه بر این کاربران می‌توانند برنامه‌های پخش شده تا دو ساعت قبل در شبکه‌ها را نیز مشاهده کنند امکان تنظیم کیفیت پخش نیز برای کاربران وجود دارد. لازم به ذکر است که تلویزیون همراه سروش، از قابلیت تصویر شناور نیز پشتیبانی می کند و کاربران می‌توانند حین تماشای تلویزیون به مکالمات خود نیز دسترسی داشته باشند.

هوش مصنوعی به کمک فرایند تشخیص چهره می آید

دانشمندان دانشگاه هنگ کنگ موفق به ساخت هوش مصنوعی شدند که می‌تواند با بررسی نقاشی بسیار ساده از چهره، تصویر اصلی آن را به صورت طبیعی بازسازی کند.

به گزارش باشگاه خبرنگاران جوان، یک الگوریتم جدید در هوش مصنوعی می‌تواند یک تصویر قابل باور از صورت افراد که به صورت خط‌خطی کشیده شده است را طراحی کند. این الگوریتم می‌تواند نحوه کشیده شدن تصاویر صورت افراد را به طور کلی تغییر دهد. گفته می‌شود پیش از اعلام نتایج اصلی این فناوری جدید هوش مصنوعی این برنامه با چهره ۱۷۰۰۰ سلبریتی آموزش دیده است.

استفاده از هوش مصنوعی برای شناسایی مظنونین

دانشمندان دانشگاه هنگ کنگ که افراد سازنده الگوریتم هوش مصنوعی مذکور هستند، ادعا می‌کنند که می‌توان از این فناوری برای شناسایی مظنونین در تحقیقات جنایی یا آسان‌تر کردن ساخت و متحرک‌سازی بازی یا فیلم استفاده کرد.

روش آموزش هوش مصنوعی برای کشیدن تصاویر واقعی چهره

بر اساس اطلاعات منتشر شده از آزمایش‌های انجام شده در این زمینه برای آموزش سیستم هوش مصنوعی، دانشمندان از تصاویر صورت افراد مشهور شروع کردند. سپس آرام آرام این تصاویر را ویرایش کردند و هر بار از پیچیدگی‌های تصویر کاسته شد، تا زمانی که دیگر به یک سری خطوط ساده رسیدند.

پس از انجام این تمرین‌ها، هوش مصنوعی یاد گرفت که خطوط موجود در یک تصویر را چگونه مانند چهره واقعی به یکدیگر متصل کند. این روش به نرم افزار کمک می‌کند بتواند با بررسی یک نقاشی ساده، چهره مورد نظر را بسازد.

مشکل موجود در هوش مصنوعی

اکنون یک مشکل در این برنامه وجود دارد. تقریبا تمام خروجی‌های ساخته شده توسط هوش مصنوعی، سفید پوست هستند.

دلیل آن هم استفاده از تصاویر افراد سفید پوست در فرایند آموزش هوش مصنوعی است. یکی از محققان دانشگاه شهر هنگ کنگ گفت که اکنون هیچ کنترلی در رنگ پوست تصاویر خروجی وجود ندارد، اما تیم توسعه دهنده آن می‌خواهد یک کنترل انعطاف پذیر برای انتخاب دستی بعضی ویژگی‌های چهره در یک پرتره اضافه کند.

توصیه‌هایی برای جلوگیری از حمله هکرها به اطلاعات کاربران دنیای مجازی

در دوره‌ای که ما میان شکاف گسترده داده‌ها قرار داریم آژانس امنیت سایبری اتحادیه اروپا توصیه‌های خود را برای بهبود امنیت رمزهای عبور و روش‌های تأیید اعتبار به اشتراک گذاشت.

به گزارش باشگاه خبرنگاران جوان، بیشتر برنامه‌هایی که برای شرکت‌ها و موسسات بزرگ و کوچک طراحی می‌شود دارای خطاها و حفره‌های برنامه نویسی هستند که این موضوع خود راه نفوذی برای هکرها می‌باشد. درنتیجه داده‌های شخصی میلیون‌ها مشتری به‌صورت آنلاین فاش می‌شوند. مجرمان سایبری باانگیزه‌ها و علایق مختلف از این داده‌ها استفاده می‌کنند تا به افراد و سازمان‌های دیگر حمله کنند. ازآنجاکه گذرواژه‌ها هنوز روشی اصلی برای تأیید اعتبار کاربران به سیستم‌عامل‌ها و دستگاه‌ها هستند، این مطلب باهدف ارائه توصیه‌های متناسب برای رعایت نکاتی از سوی کاربران دنیای مجازی جهت مقابله با حمله هکرها ارائه می‌گردد.

خطرات گذرواژه‌ها

امروزه کلمه عبور (پسورد) می‌تواند به چندین روش سرقت شود، از جمله:

۱- حملات مهندسی اجتماعی مانند فیشینگ با استفاده از صفحات جعلی و فیشینگ صوتی به اصطلاح (Vishing) که از ترکیب دو کلمه Voice و Phishing ساخته‌شده است.

زمانی که کلاه‌برداری از سرور صوتی تعاملی یا پیام صوتی برای تماس با کاربران و باهدف ربودن اطلاعات شخصی و خصوصی آن‌ها استفاده می‌کند به آن Vishing می گویند. هدف همانند همان فیشینگ است که با ایمیل یا Smishing با اس ام اس انجام می‌شود.

معمولاً Vishing پیامی به‌ظاهر فوری است و از کاربر درخواست می‌شود که سریعاً عمل کند. مطمئناً هرگز به این‌گونه تماس‌ها نباید اهمیت داده‌شده و جدی گرفته شوند.)

۲- سرقت اطلاعات با استفاده از نرم‌افزارهای تخصصی یا

کلیدهای برقی فیزیکی.برخی از این حملات به حضور فیزیکی یا نزدیکی با لپ‌تاپ یا دستگاه نیاز دارند. با متوقف کردن ارتباطات استفاده از نقاط دستیابی جعلی یا اعمال فشار حملات (MiTM)در رمزنگاری و امنیت رایانه شکلی از استراق سمع فعال است که در آن حمله‌کننده یا همان هکر اتصالات مستقلی را با قربانیان برقرار می‌کند و پیام‌های مابین آن‌ها را شنود و بازپخش می‌کند، به‌گونه‌ای که آن‌ها را معتقد کند که با یکدیگر به‌طور مستقیم در طول یک اتصال خصوصی، صحبت می‌کنند؛ درحالی‌که تمام مکالمات توسط حمله‌کننده کنترل می‌شود.)

در سطح شبکه، در WiFiهای عمومی که در هتل‌ها، کافه‌ها فرودگاه‌ها و ... مشاهده می‌شود، شیوع بیشتری دارد.

توصیه‌هایی برای بهبود امنیت رمز عبور

قابلیت تأیید اعتبار چند فاکتوری، حالت (دومرحله‌ای) را در هر زمان ممکن برای همه حساب‌های خود فعال کنید از رمزهای عبور خود مجدداً بر روی سایر اپلیکیشن‌ها استفاده نکنید.

بزهکاران سایبری با این فرض کار می‌کنند که بسیاری از کاربران از رمزهای عبور مجدد استفاده نمی‌کنند، ازاین‌رو میزان موفقیت بالایی که در تعیین رمزها استفاده کرده‌اید به خطر می‌افتد. به‌منظور کاهش این ریسک، از قابلیت‌های ورود به سیستم با تأیید هویت چندمرحله‌ای استفاده کنید.

از یک مدیر کلمه عبور استفاده کنید

مدیر کلمه عبور یا پسورد منیجر (Password Manager) به ابزاری گفته می‌شود که امکان ایجاد و بازیابی کلمه‌های عبور را برای کاربر فراهم می‌کند. معمولاً کلمه‌های عبور کاربر با کمک چنین ابزارهایی در یک پایگاه داده رمزنگاری‌شده محلی یا آنلاین نگه‌داری می‌شود و کاربر تنها با به خاطر سپردن یک کلمه عبور اصلی (موسوم به Master Password که برای استفاده از این ابزار تعیین می‌کند می‌تواند به تمام کلمات عبور و اطلاعات ذخیره‌شده دسترسی پیدا کند بر اساس آخرین دستورالعمل‌های موجود، برای هر وب‌سایت و خدمات مجزا رمزهای عبور و منحصربه‌فرد ایجاد کنید.

اینجاست که مدیریت رمز عبور خود را مفید جلوه می‌دهد بررسی کنید که آیا ممکن است حساب‌ها و اطلاعات شما بنا به امنیتی که برایشان تعریف کرده‌اید به خطر بی افتد یا نه، در صورت مثبت بودن جواب بلافاصله با تغییر رمزهای عبور خود برای سرویس‌های مشخص‌شده اقدام کنید، بسیاری از وب‌سایت‌ها ویژگی‌های یادآوری رمز عبور را ارائه می‌دهند. اطمینان حاصل کنید که برای تعیین مجدد گذرواژه‌تان، مثلاً به اطلاعات شخصی راحت و قابل حدس اعتماد نکنید. مانند استفاده از نام حیوان خانگی، تاریخ تولد، نام دبیرستان و ...

هنگام دسترسی به بانکداری الکترونیکی یا سایر خدمات خصوصی از WiFi عمومی، از VPN یا حداقل نقاط دسترسی تلفن همراه استفاده کنید، از محیط اطراف خود در سالن‌ها، فرودگاه‌ها قطارها و کافه‌ها آگاه باشید و اطمینان حاصل کنید که هیچ کس در پشت شما نیست اینجاست که حفظ حریم خصوصی معنی پیدا می‌کند.

باج‌افزاری که دانش آموزان را هدف قرار داده است

بر اساس جدیدترین اخبار منتشر شده، باج‌افزار STOP/Djvu در سطح کشور در حال گسترش است.

+به گزارش باشگاه خبرنگاران جوان، باج‌افزار STOP برای نخستین بار در تاریخ ۲۵ دسامبر ۲۰۱۷ میلادی مشاهده گردید. این باج‌افزار تاکنون با اسامی مختلفی از جمله STOP، Djvu، Drume و STOPData در فضای سایبری معرفی شده است. اما به طور کلی به دو دسته STOP و Djvu تقسیم می‌گردد. Djvu در واقع نسخه جدیدتر این باج‌افزار بوده که از نظر عملکرد شبیه والد خود (STOP) می‌باشد و امروزه آن‌ها را با نام STOP/Djvu می‌شناسند. تعدد نسخه‌ها در فواصل زمانی کوتاه در واقع تکنیکی است که باج‌افزار STOP/Djvu از آن برای نفوذ و اثرگذاری بیشتر استفاده می‌کند. تاکنون بیش از ۲۰۰ پسوند مختلف از این باج‌افزار مشاهده گردیده است. بر اساس آمارهای منتشر شده در وب‌سایت Emsisoft تنها در سه‌ماهه اول ۲۰۲۰ بیش از ۶۶۰۹۰ مورد گزارش آلودگی به این باج‌افزار توسط قربانیان به ثبت رسیده است. این رقم حدوداً ۷۰٪ از موارد آلودگی به باج‌افزارها در سطح جهان را به خود اختصاص داده است. نسخه‌هایی از این باج‌افزار با پسوندهای alka nbes، redl، kodc، topi، righ، bboo، btos و ... در کشور ایران نیز مشاهده شده است.

باج‌افزار STOP/Djvu با زبان برنامه‌نویسی C++ نوشته شده است. نسخه‌های جدید این باج‌افزار در کد نویسی خود به شدت مبهم‌سازی (Obfuscate) شده‌اند و از انواع روش‌های anti-emulation و anti-debugging برای جلوگیری از تحلیل توسط تحلیل گران بدافزار استفاده کرده‌اند. برخی از نسخه‌های این باج‌افزار نیز باتوجه به منطقه زمانی و موقعیت جغرافیایی میزبان فرآیند رمزگذاری را انجام می‌دهند و بدین ترتیب به صورت هدفمندتر قربانیان خود را انتخاب می‌کنند.

این باج‌افزار به محض اجرا در سیستم قربانی ابتدا یک نسخه از فایل اجرایی خود را در مسیر "AppData%Local%" کپی کرده و با افزایش سطح دسترسی خود به کاربر Administrator و اجرای دستوراتی در محیط CMD با سرور فرمان و کنترل (C &C)

خود ارتباط می‌گیرد و فایل‌ها را با کلید آنلاین و الگوریتم نامتقارن RSA-۲۰۴۸ رمزگذاری می‌کند. در برخی نسخه‌ها از الگوریتم Salsa۲۰ نیز برای رمزگذاری فایل‌ها استفاده شده است. در صورتی که باج‌افزار به هر دلیل موفق به برقراری ارتباط با سرور خود نگردد از روش آفلاین (الگوریتم AES-۵۲۶) برای رمزگذاری فایل‌ها استفاده می‌کند. نسخه‌های اولیه این باج‌افزار از روش آفلاین برای رمزگذاری فایل‌های قربانیان استفاده می‌کردند و شرکت‌هایی مثل Emsisoft توانستند برای این نسخه‌ها رمزگشا ارائه دهند. اما از آگوست ۲۰۱۹ شیوه رمزگذاری باج‌افزار STOP/Djvu تغییر کرد و در حال حاضر تنها به روش آنلاین رمزگذاری را انجام می‌دهد؛ لذا بدون کلید خصوصی مهاجم که در سرور (C &C) باج‌افزار ذخیره شده است عملاً رمزگشایی فایل‌ها غیرممکن خواهد بود. در مواردی مشاهده شده که باج‌افزار STOP/Djvu پس از ارتباط با سرور (C &C) سیستم قربانی را به انواع تروجان‌ها و جاسوس‌افزارها از قبیل Vidar و Azorult که اطلاعات حساس سیستم قربانی را سرقت می‌نماید نیز آلوده نموده است؛ لذا توجه به این نکته در زمان ارائه خدمات امداد به قربانیان این باج‌افزار ضروری است.

باج‌افزار STOP/Djvu برای جلوگیری از شناسایی و دور زدن آنتی‌ویروس‌ها به صورت مداوم پسوند و ساختار خود را تغییر می‌دهد. به همین دلیل است که حتی از سد به‌روزترین آنتی‌ویروس‌ها نیز عبور می‌کند. بر اساس گزارش‌های رسیده از قربانیان این باج‌افزار در سرتاسر جهان، باج‌افزار STOP/Djvu معمولاً از طریق کرک و فعال‌سازهای ویندوز KMSAuto، KMSPico، آفیس و سایر نرم‌افزارها (از قبیل اتوکد، فتوشاپ، دانلود منیجر و ...) و همچنین لایسنس‌های تقبلی و حتی آپدیت‌های جعلی ویندوز منتشر می‌شود. نسخه‌هایی از این باج‌افزار حتی در قالب اسناد آفیس و فایل Setup نرم‌افزارهای مرتبط با پایان‌نامه‌ها جاسازی شده و قشر دانشجو را مورد هدف قرار داده است. باتوجه به موارد فوق می‌توان این‌گونه نتیجه‌گیری کرد که جامعه هدف باج‌افزار STOP/Djvu کاربران شخصی و خانگی بوده و برای سرورها و سازمان‌ها تهدید کمتری محسوب می‌گردد؛ بنابراین اطلاعات از دست رفته ارزش مادی بالایی ندارند. دلیل آن هم روش انتشار این باج‌افزار می‌باشد که بیشتر مبتنی بر دانلود فایل‌های آلوده در اثر بی احتیاطی کاربران است. طبق بررسی‌های صورت گرفته، می‌توان گفت که رفتار باج‌افزار STOP/Djvu در کشور ایران به صورت فصلی می‌باشد. در فصولی که دانشجویان به دنبال یافتن قالب برای پایان‌نامه‌ها یا سایر مقالات و ارائه‌های خود هستند، رخدادهای بیشتری مشاهده می‌گردد.

به منظور پیشگیری از آلودگی و مقابله با این باج‌افزار توصیه می‌گردد در مرحله اول سیستم‌عامل، آنتی‌ویروس و سایر نرم‌افزارها به صورت مداوم به‌روزرسانی گردند. همچنین کاربران می‌بایست از دانلود هرگونه فایل یا نرم‌افزار از وب‌سایت‌های ناشناس خودداری کرده و قبل از اجرای فایل‌ها بر روی سیستم خود حتما آن‌ها را با آنتی‌ویروس‌های به‌روز و سامانه‌های آنلاین مثل VirusTotal اسکن نمایند. در پایان یادآور می‌گردد که پشتیان‌گیری منظم از اطلاعات به صورت آفلاین تنها راه قطعی مقابله با هرگونه تهدید سایبری خصوصاً باج‌افزارهاست.

استفاده از دوربین شش گانه متحرک در گوشی Galaxy S۳۰

به تازگی اختراع جدیدی از سامسونگ به ثبت رسیده که نشان می‌دهد این شرکت قصد دارد از دوربین شش گانه متحرک در پرچمدار بعدی خود استفاده کند.

به گزارش باشگاه خبرنگاران جوان، به تازگی طرح اولیه‌ای از یکی از گوشی‌های آینده سامسونگ که انتظار می‌رود Galaxy S۳۰ باشد منتشر شده است که نشان می‌دهد سامسونگ قصد دارد در این گوشی تمرکز خاصی روی دوربین داشته باشد. بر اساس پتنت منتشر شده از این گوشی ظاهرا سامسونگ قصد دارد از دوربین شش گانه برای این اسمارت فون استفاده کند تا از این طریق تصاویری بسیار با جزییات بالا به ثبت برسند.

اطلاعات منتشر شده ظاهرا به واسط ثبت اختراع جدید سامسونگ در حوزه تلفن‌های هوشمند فاش و پس از بررسی این اطلاعات توسط متخصصان مشخص شد که سامسونگ قصد استفاده از دوربین شش گانه را در پرچمدار بعدی خود دارد. اما موضوع بسیار جالب در بخش دوربین این گوشی، به قابلیت حرکت و کج شدن هر کدام از این شش لنز مربوط می‌شود که به ای ترتیب بازه وسیع‌تری از محیط در قاب دوربین به ثبت خواهد رسید.

طبق ثبت اختراع جدید سامسونگ، این شرکت برای قرار دادن این شش لنز در کنار یکدیگر مجبور است تا همه‌ی آن‌ها را به صورت افقی در کنار یکدیگر قرار دهد تا فضای زیادی از پشت گوشی اشغال نشوند؛ در حال حاضر هر شش لنز در قسمت پشت و بالای این گوشی قرار دارند.

پنج مورد از شش لنز استفاده شده در این گوشی از قابلیت زاویه دید عریض بهره می‌برند اما یکی از این پنج لنز به عنوان لنز اصلی خواهد بود و از کیفیت بالاتری نسبت به سایر لنزها برخوردار است؛ لنز ششم نیز برای عکس برداری فوتو مناسب خواهد بود. ثبت اختراع جدید سامسونگ pano-bokeh نام گذاری شده است که از آن هنوز در هیچ تلفن همراهی در بازار استفاده نشده است و ساسونگ قصد دارد اولین شرکت سازنده گوشی با دوربین متحرک در جهان باشد. با این حال برای کسب اطلاعات بیشتر باید تا زمان اعلام رسمی شرکت سامسونگ منتظر ماند.

پردازنده‌های Ryzen ۴۰۰۰ جانشین Ryzen Zen۳ خواهند شد

شرکت AMD اعلام کرده پردازنده‌های Ryzen۴۰۰۰ نسل بعدی پردازنده‌های رده بالای این شرکت خواهند بود.

به گزارش باشگاه خبرنگاران جوان، شرکت AMD یکی از قدیمی‌ترین شرکت‌های سازنده پردازنده‌های موبایل است که قدرتمندترین پردازنده در دسترس از این شرکت همان پردازنده نسل سوم Ryzen Zen۳ است. این پردازنده در سال ۲۰۱۹ وارد بازار شد و توانست انقلابی بزرگ در صنعت سخت افزار برپا کند. اما شرکت AMD به تازگی نسل بعدی پردازنده خود که AMD Ryzen ۴۰۰۰ نام دارد را معرفی کرده و قصد دارد این نسل از پردازنده را جایگزین نسل Ryzen Zen۳ کند؛ به نوعی می‌توان گفت نسل جدید پردازنده‌های AMD همان پردازنده‌های Ryzen Zen۳ هستند که شرکت سازنده سعی کرده است آن‌ها را ارتقا داده و وارد بازار کند.

شرکت AMD درباره این دو پردازنده اعلام کرده است که پردازنده‌های جدید این شرکت و همچنین کارت‌ها گرفیک RDNA۲ از اواخر سال جاری در دسترس کاربران قرار خواهد داشت که بر اساس سابقه شرکت AMD انتظار می‌رود این محصولات در نمایشگاه فناوری Computex برای اولین بار عرضه شوند. هر این نمایشگاه ابتدا برای ماه سپتامبر برنامه ریزی شده بود اما به دلیل شیوع ویروس کرونا در جهان، برگزاری مراسم مذکور تا اواخر سال جاری به تاخیر افتاد و در صورتی که وضعیت ویروس کرونا در جهان بهبود نداشته باشد همچنان این نمایشگاه عقب خواهد افتاد.

از طرفی هم شاید بتوان گفت نسل آخر پردازنده‌های سری Ryzen Zen۳ عملکردی بالاتر از سری ۴۰۰۰ داشته باشند چرا که AMD بارها مشکلات موجود در این نسل را برطرف کرده است و می توان گفت این نسل از پردازنده به ثبات قابل قبولی رسیده است.

در بخش قیمت نیز انتظار می‌رود پردازنده ۱۶ هسته‌ای جدید AMD قیمتی حدود ۲۵ درصد بیشتر از سری Ryzen Zen۳ داشته باشد، اما هنوز قیمت دقیق این محصول از سوی AMD اعلام نشده است.