خبر

جبران کمبود پهنای باند اینترنت با شبکه توزیع محتوا

● **مهر:** شبکه‌های توزیع محتوا در جهت جبران کمبود پهنای باند اینترنت عمل می‌کنند. از آنجایی که کاربران در ایران از سرعت پایین اینترنت شکایت دارند، یکی از راهکارهای مهم برای حل این مسئله شبکه توزیع محتوا است. شبکه‌های توزیع محتوا (CDN) و ابرهای امنیتی به خدماتی گفته می‌شود که برای افزایش امنیت، سرعت و کارایی محتوای تحت وب فعالیت می‌کنند؛ خدماتی که در چند سال اخیر، با وجود پیچیدگی‌های تکنولوژیک فراوان، سرمایه‌گذاری‌های چند ده‌میلیون‌دلاری را جذب کرده‌اند. در حال حاضر، شرکت‌های زیادی در دنیا خدمات ابری ارائه می‌دهند و هر روز تعداد آنها، بیشتر و بیشتر می‌شود و براین‌اساس، در ایران نیز برای اولین‌بار قرار است این شبکه راه‌اندازی شود. افزایش سرعت بارگذاری صفحات و محتوا یکی از نتایج به کارگیری این خدمت است. شبکه‌های CDN به کمک تنظیمات DNS، بین کاربران اینترنتی و سرور سرویس‌دهنده قرار می‌گیرد و کارایی و بازدهی سایت را به‌شدت ارتقا می‌دهد. از سوی دیگر، این شبکه‌ها برای جبران کمبود پهنای باند اینترنت عمل می‌کنند و از آنجایی که کاربران در ایران از سرعت پایین اینترنت هنگام استفاده از وبسایت‌ها شکایت دارند، یکی از راهکارهای مهم برای حل این مسئله، شبکه‌های توزیع محتوا (CDN) یا همان سرویس‌دهی خدمات ابری در سطح مناطق مختلف جغرافیایی است.

نفوذ به پایانه‌های فروش

● **شبکه‌گستر:** گروهی از نفوذگران حرفه‌ای با بهره‌گیری از ابزارهای قابل استفاده در آزمون‌های نفوذپذیری و با هدف آلوده‌کردن پایانه‌های فروش (PoS) و سرقت اطلاعات کارت‌های بانکی، شرکت‌های کوچک و متوسط را هدف قرار داده‌اند. براساس گزارش شرکت ضدویروس Trend Micro، این نفوذگران ابتدا با اجرای حملات لغت‌نامه‌ای (Dictionary Attack) و حملات جست‌وجوی فراگیر (Brute-force Attack) به جمع‌آوری اطلاعات اصالت‌سنجی کامپیوترهای با گذرواژه ضعیف در بستر اینترنت اقدام می‌کنند. در مرحله بعد، با اجرای ابزارها و سرویس‌های مجاز نصب شده بر این سیستم‌ها همچون VNC Viewer، وRemote Desktop Protection و Remote Desktop Connection به دستگاه متصل شده و به یافتن پایانه‌های فروش موجود در شبکه اقدام می‌کنند. نفوذگران Black Atlas به‌محض دست‌یافتن به پایانه‌های فروش، اطلاعات ذخیره شده بر روی RAM دستگاه کارت‌خوان را که حاوی اطلاعات کارت بانکی متصل‌شده به آن است، سرقت می‌کنند. با توجه به اینکه بدافزار BlackPOS توانایی ارسال آنلاین داده‌های جمع‌آوری‌شده را ندارد و جزئیات کارت را تنها بر یک فایل متنی ذخیره می‌کند، نفوذگران Black Atlas آن را با یک درب پشتی (Backdoor) با نام Gorynych ترکیب کرده‌اند. این درب پشتی اطلاعات فایل متن را با روش HTTP POST به سرورهای فرماندهی نفوذگران ارسال می‌کند. این نفوذگران علاوه‌بر آلوده‌کردن پایانه‌های فروش و سرقت اطلاعات اصالت‌سنجی کارت‌های متصل‌شده به آنها، گذرواژه‌های ایمیل و Face-book را نیز جمع‌آوری می‌کنند. کشورهای آمریکا، استرالیا، هند، تایوان، آلمان و انگلیس بیش از سایر کشورها هدف Black Atlas قرار گرفته‌اند.

یاهو همدستی دولت‌ها با هکرها را افشا می‌کند

● **فارس:** با افزایش حملات هکرها و خرابکاران اینترنتی، برخی شرکت‌های فناوری از برنامه‌های خود، برای آگاه‌ساختن کاربران از این نوع حملات خبر داده‌اند. براساس گزارش دیجیتال ترندز، یاهو تازه‌ترین شرکتی است که اعلام کرده برای ایمن‌سازی سایت و خدمات خود به کاربرانش درباره حملات هکرهایی که دولت‌ها آنها را حمایت می‌کنند، هشدار خواهد داد. باب لرد، مدیر امنیت اطلاعات یاهو، دراین‌باره گفته است: یاهو درصورت مظنون‌شدن به هدف قرارگرفته‌شدن حساب کاربری هر یک از کاربرانش، آنها را از این موضوع آگاه خواهد کرد. او افزوده است که این شرکت به‌دنبال انجام اقدامات جدیدی برای حفاظت از حساب‌های کاربری مشترکان خود و مقابله با حملات پیچیده روزافزون هکری است. به دنبال افشاگری‌های ادوارد اسنودن درباره همدستی دولت آمریکا با شرکت‌های فناوری این کشور برای جاسوسی از میلیون‌ها کاربر اینترنت، این شرکت‌ها برای حفظ آبرو و اعتبار خود و ازدست‌ندادن سود و درآمد اقتصادی درصدد برآمده‌اند با ارائه خدماتی از این دست اعتماد مردم را مجددا جلب کنند. اولین‌بار گوگل اعلام کرد قصد دارد کاربران را از حملات هکری‌ای که از سوی دولت‌ها حمایت می‌شوند آگاه کند و پس از آن توییتر و فیس‌بوک هم مدعی ارائه خدماتی از این دست شده و به کاربرانی که با حمله هکرها روبه‌رو می‌شدند، ایمیل‌های هشدارآمیزی ارسال کردند.

مؤسسه انگلیسی BMI:

بازار آی‌تی ایران در دستور کار شرکت‌های آمریکایی

پس از توافق هسته‌ای، هر روز شاهدیم نام یکی از شرکت‌های آمریکایی با عنوان اینکه قصد فعالیت جدی‌تری در ایران دارد، مطرح می‌شود. معروف‌ترین آنها نیز مایکروسافت و اپل بودند. البته دراین‌میان برخی نام‌های دیگر مانند HP و جنرال‌الکتریک نیز دیده می‌شد. پیش‌تر نیز محمدرضا طلایی، رئیس مجمع تشکل‌های فناوری ایران از ملاقات‌های مسئولان ایرانی فناوری اطلاعات با برندهای معتبر دنیا در نمایشگاه جیتکس امارات خبر داده بود. دراین‌باره محسن جلال‌پور، رئیس اتاق تهران نیز در جریان حضور غرفه ایران در نمایشگاه جیتکس امارات گفته بود: «اینکه دقیقا چه تعداد برند خواستار ورود به بازار ایران هستند، محاسبه‌کردنی نیست، اما حداقل می‌توان گفت نمایندگان اوراکل، آی‌بی‌ام و ودافون، مایکروسافت، اپل، جماتلو، جکیز بیزنس، سولوشن، فاموکو، فالو سافت و بیزنس فرانس خواستار حضور در بازار ایران با قبول همکاری در زمینه انتقال دانش فنی شدند». به نوشته «وال‌استریت ژورنال»، شرکت‌های بزرگ آمریکایی خود را برای ورود به بازار ایران پس از برداشته‌شدن تحریم‌ها آماده می‌کنند. به نوشته این روزنامه، شرکت‌های بزرگ آمریکایی، ازجمله تولید تجهیزات رایانه‌ای «اچ‌پی» و «جنرال‌الکتریک»، فعالانه در حال بررسی ورود به بازار ایران، در آستانه رفع تحریم‌ها علیه این کشور هستند. درحالی‌که شرکت‌های آمریکایی، غیر از شرکت‌های غذایی، قطعات یدکی هواپیما و تجهیزات پزشکی، همچنان از انجام مبادلات مستقیم مالی با ایران منع شده‌اند. یک مقام دولت آمریکا

می‌گوید اداره کنترل دارایی‌های خارجی وزارت خزانه‌داری آمریکا در روز «اجرای برجام»، با صدور مجوزی به بخش‌های امور خارجی‌های آمریکا اجازه فعالیت‌های اقتصادی با ایران را خواهد داد. در همین راستا به‌تازگی مؤسسه تحقیقاتی BMI مستقر در انگلستان گفته است: شرکت‌های آمریکایی رسما ورود به بازار آی‌تی ایران را در دستور کار خود قرار داده و به‌زودی شاهد حضور رسمی شرکت‌هایی مانند اچ‌پی و اپل خواهیم بود. براساس پیش‌بینی این مؤسسه، بازار رایانه، موبایل و گیم در ایران از رقم ۹،۵ میلیارد دلار در سال ۲۰۱۴ به رقم ۱۳ میلیارد دلار خواهد رسید و جمعیت ۷۷میلیونی ایران پتانسیل حضور بزرگان آی‌تی دنیا را در خود دارد. از سوی دیگر شرکت‌های آسیایی و اروپایی که منتظر برداشته‌شدن رسمی تحریم‌ها نشده‌اند، سعی کرده‌اند به صورت خزنده وارد بازار ایران شوند و به همین دلیل شرکت‌های آمریکایی از این بابت احساس نگرانی کرده‌اند که مبادا بازار جدیدی مثل ایران را برای همیشه از دست بدهند. بر همین اساس، شرکت HP Sarl که شعبه سوئیسی اچ‌پی آمریکاست، ماه گذشته موافقت‌نامه رسمی با مقامات ایرانی در زمینه فروش محصولات سخت‌افزاری و پشتیبانی فنی از سرورهای اچ‌پی را (که در ایران بسیار محبوب بوده و در دوران تحریم نیز دور زده می‌شده) امضا کرده تا بتواند فروش رسمی محصولاتی مانند تبلت، لپ‌تاپ و... را به‌زودی در ایران راه‌اندازی کند. اپل نیز از طریق شعبه‌های خود در اروپا با مقامات ایرانی ارتباط پیدا کرده تا زمینه فعالیت رسمی و حتی دایرکردن فروشگاه رسمی را بررسی کند. هرچند حضور مستقیم اپل در ایران به ضرر فروشندگان و توزیع‌کنندگان ایرانی است و ممکن است فروش مستقیم تبدیل به فروش غیرمستقیم از طریق توزیع‌کنندگان شود، اما موضوع خدمات پس از فروش، دغدغه هر دو طرف است که تا این موضوع حل نشود، حضور رسمی و مستقیم صورت نخواهد گرفت. با وجود اینکه تاکنون اقدام رسمی از سوی هیچ‌یک از شرکت‌های خارجی برای حضور در ایران نشده است، اما در هفته اخیر برخی نمایندگان کشورهای خارجی در نمایشگاه الکامپ حضور یافتند تا از نزدیک به ارزیابی فضای ایران بپردازند.

تغییر سطح رمزگذاری سبب می‌شود

محدودیت دسترسی به اینترنت برای میلیون‌ها نفر

درحال‌حاضر کاربران اینترنتی ممکن است قفل کوچک سبزرنگ یا طلایی‌رنگی را در گوشه نوار آدرس مرورگر اینترنتی خود مشاهده کنند اما از تاریخ یکم ژانویه سال ۲۰۱۶، این قفل رنگی برای درصد کمی از کاربران اینترنتی سراسر جهان ناپدید خواهد شد و در ادامه میلیون‌ها کاربر، دسترسی خود به وب‌سایت‌های مختلف را از دست خواهند داد. این فرایند، ارتباط مستقیمی با اصطلاح «SHA-1 Sunset» (کلیدواژه مورداستفاده اهل فن برای تشریح انقضای پشتیبانی از سطح خاصی از رمزگذاری) دارد. درواقع در سال آینده میلادی، الگوریتم‌های قدیمی‌تر از سطح رمزگذاری SHA-1 دیگر نیازهای لازم امنیتی برای وب‌سایت‌ها را برآورده نخواهند کرد و از همین رو بر اساس تحقیقات انجام‌شده از سوی شرکت امنیتی CloudFlare چیزی در حدود ۳۳ میلیون نفر در سراسر دنیا، دسترسی خود به این وب‌سایت‌ها را از دست خواهند داد. این فرایند، به‌روزرسانی‌ای متداول برای قابلیت‌های امنیتی تحت وب است اما این تغییر که توسط کنسرسیوم تولیدکنندگان نرم‌افزاری مرورگرهای اینترنتی اتخاذ شده، می‌تواند استفاده کاربران از اینترنت گوشی‌های هوشمند در کشورهای درحال‌توسعه را به‌شدت تحت‌تاثیر قرار دهد. در نتیجه این امر، قسمتی از جمعیت آسیب‌پذیر دنیا با مجموعه‌ای از وب‌سایت‌هایی که نیاز به این پروتکل‌های امنیتی ندارند، تنها خواهند شد. به گزارش آی‌تی ایران، تیم ارلین، مسئول قسمت امنیتِ آی‌تی در شرکت تریپ‌وایر درباره فرایندهای جدید امنیتی، توضیحات کاملی ارائه کرده است. او دراین‌باره می‌گوید: «وقتی وب‌سایت شما با مرورگر اینترنتی، ارتباط برقرار می‌کند، فرایند ارسال و دریافت داده‌ها انجام خواهد شد. در طول فرایند رمزگذاری، وب‌سایت و مرورگر وارد مکالمه‌ای بر پایه استفاده از استعارات خاص خواهند شد. در این روند، از کدهای محرمانه و ایمن برای گفت‌وگو استفاده خواهد شد که متفاوت از گفت‌وگوهای معمولی است. قسمتی از ارتباطات بین مرورگر و وب‌سایت به توافق بر سر استفاده از پیچیده‌ترین زبانی که هر دو طرف توانایی فهم آن را داشته باشند، اختصاص خواهد یافت. نفوذگران می‌توانند این الگوریتم را بشکنند و مکالمات موجود را شنود کنند. بنابراین همواره باید برنامه‌ای برای به‌روزرسانی این الگوریتم‌ها وجود داشته باشد». خوشبختانه وب‌سایت‌ها و مرورگرهای زیادی وجود دارند که به‌طور پیش‌فرض از نسخه‌های رمزگذاری‌شده در قالب پسوند s و آدرس‌های https://// استفاده می‌کنند و به همین دلیل در صورتی که شما از مرورگری به‌روزرسانی‌شده استفاده کنید، احتمالا به طور خودکار حداقل به سطح SHA-2 الگوریتم‌های امنیتی، ارتقا داده شده‌اید. با توضیحات بالا، مرورگرها و سیستم‌عامل‌های قدیمی‌تر مانند ویندوز ایکس‌پی احتمالا از به‌روزرسانی‌های جدید رمزگذاری پشتیبانی نخواهند کرد. از سوی دیگر، فرایندهای جدید رمزگذاری به توان پردازشی بیشتری نیاز خواهد داشت و همین امر باعث خواهد شد گوشی‌های همراه قدیمی که اکثرا در کشورهای درحال‌توسعه، استفاده می‌شوند، امکان استفاده از مرور امن در فضای وب را از دست بدهند. همین امر باعث خواهد شد کاربرانی که از گوشی‌هایی با عمر پنج سال به بالا استفاده می‌کنند، با پیغام خطایی هنگام درخواست برای مشاهده وب‌سایت‌هایی که نسخه‌های رمزگذاری‌نشده ارائه نمی‌دهند، روبه‌رو شوند. این در حالی است که شرکتی مانند گوگل، پافشاری بیشتری برای غیرفعال‌کردن پشتیبانی از قابلیت‌های رمزگذاری قدیمی دارد. شرکت‌هایی مانند علی‌بابا هم اعلام کرده‌اند همچنان از نسخه‌های قدیمی‌تر رمزگذاری اینترنتی پشتیبانی خواهند کرد تا طیف گسترده‌تری از کاربران بتوانند دستگاه‌های خود را ارتقا دهند.

امنیت

ایران و جنگ‌های سایبری

● پس از کشف و شناسایی بدافزار Flame، حملات سایبری همچنان ادامه دارد. انتشار بدافزار پیچیده بانکی Gauss در اواسط سال ۹۱، عملیات جاسوسی Mask در اواخر سال ۹۲ و بدافزار Regin در سال ۹۳ تنها بخش کوچکی از حملات سایبری است که در بین این سال‌ها ایران آنها را تجربه کرده است. وضعیت امنیتی شبکه‌های ایران مستحکم‌تر از سال ۹۱ شده و به این حملات واکنش به‌موقع نشان داده می‌شود. در بهمن ۱۳۹۳ شرکت کسپراسکی گزارشی منتشر می‌کند و در آن به معرفی گروهی نفوذگر به نام Equation می‌پردازد. کلمه Equation اقتباس شده از الگوریتم رمزگذاری و روش‌های مخفی‌سازی این گروه است. روش‌ها و ابزارهای استفاده شده از سوی گروه Equation بی‌نظیر و منحصربه‌فرد است.

عملیات جاسوسی و سرقت اطلاعات به وسیله این گروه در بیش از ۳۰ کشور جهان، ازجمله ایران گسترده بوده و از سال ۲۰۰۱ میلادی و حتی شاید ۱۹۹۶ میلادی آغاز شده است. گرچه شرکت کسپراسکی از سازمان امنیت ملی آمریکا ان‌اس‌اِی (NSA) به عنوان طراح و گرداننده این عملیات نام نبرده و آن را فقط به گروه Equation نسبت می‌دهد، اما شواهد متعددی از وجود چنین ارتباطی خبر می‌دهد. یکی از شواهد این ارتباط بدافزار Fanny است که از سال ۱۳۸۷ به وسیله گروه Equation استفاده شده است و از جهاتی شباهت به بدافزار مشهور استاکس‌نت دارد. بدافزار Fanny از طریق حافظه‌های USB Flash منتشر می‌شود و هدف اصلی آن جمع‌آوری و سرقت اطلاعات است. تمرکز فعالیت Fanny روی شبکه‌های بسته و به‌دور از اینترنت است. به چند نکته درباره بدافزار Fanny باید توجه ویژه داشت:

۱- این بدافزار از نقطه ضعفی برای انتشار خود استفاده می‌کرده که بدافزار استاکس‌نت هم بعدا عینا از آن بهره برده است. بدافزار Fanny از سال ۱۳۸۷ از این ضعف امنیتی استفاده می‌کرده است. حال آنکه اولین گونه از بدافزار استاکس‌نت مربوط به سال ۱۳۸۹ می‌شود. همچنین بدافزار Fanny از یک نقطه‌ضعف ناشناخته دیگر در سیستم‌عامل ویندوز استفاده می‌کرده که در برخی گونه‌های استاکس‌نت هم مشاهده شده است.

بازار

نبرد برندها در بازار موبایل

سال ۲۰۱۵ میلادی هم رو به پایان است. امسال برندهای مختلف، تلفن‌های پرچمدار خود را روانه بازار کردند که هر یک مزایا و معایب خود را داشتند. آنچه در صنعت موبایل امسال رخ داد، کمترشدن فاصله رقبای اندرویدی، ادامه روند روبه‌رشد ویندوزفون و تداوم موفقیت‌های آیفون بود. همچنین شاهد اوج‌گرفتن تولیدکننده‌های چینی، مثل هوآوی، اوپو و شیائومی بودیم که محصولاتی درخور و بسیار باکیفیت را روانه بازار کردند.

V10 یا اکسپریا زد۵ پریمیوم

به گزارش زومیت، ال‌جی در گوشی هوشمند V10 خود از ترکیب پلاستیک فشرده و فریم فلزی استفاده کرده است و همچنان دکمه‌های کنترل صدا و پاور نیز در پشت دستگاه قرار داده شده‌اند، با این تفاوت که حسگر اثر انگشت با دکمه پاور یکپارچه شده است تا کاربران این گوشی بتوانند قفل گوشی را از طریق این سنسور باز کنند. در V10 نه‌تنها در حالت عکاسی قادر هستید پارامترهای عکاسی را تحت کنترل کامل خود بگیرید، بلکه برای اولین‌بار در دنیای موبایل، ال‌جی امکان اعمال تنظیمات دستی در حالت فیلم‌برداری را نیز میسر کرده است. سونی در جریان نمایشگاه IFA 2015 از سه گوشی هوشمند پرچمدار خود با نام‌های Xperia Z5، Xperia Z5 Compact و Xperia Z5 Premium رونمایی کرد. دو گوشی اول جایگزین نسل قبلی خود شدند، اما گوشی پرهیاهوی سونی در برلین، اکسپریا زد۵ پریمیوم بود. این گوشی حداقل از یک جنبه بی‌همتاست. فبلت امسال سونی به صفحه‌نمایش 4K مجهز شده است که تراکم خارق‌العاده ۸۰۶ پیکسل در اینچ را ارائه می‌کند. تراکم پیکسلی که تا پیش از این در هیچ گوشی هوشمندی وجود نداشته است.

Iphone6+ یا نکسون

از سویی دیگر آیفون۶اس پلاس برای طرفداران گوشی‌هایی با نمایشگر بزرگ تولید شده است. این گوشی در رنگ جدید رز گلد (صورتی) نیز عرضه می‌شود. اپل در آیفون‌های جدید از فناوری فورس‌تاچ و یک فناوری جدید با نام D Tiuch3 نیز بهره گرفته و علاوه‌براین، از آلیاژ جدیدی نیز استفاده کرده است. به لطف وجود فورس‌تاچ، آیفون به ژست‌های جدید Peek و Pop و موتور تپتیک مجهز شده است. گوگل برای اولین‌بار به معرفی دو نکسوس پرداخته است که تولید یکی از این دستگاه‌ها به هوآوی سپرده شده است. این گوشی ۵،۷اینچی به همراه آخرین نسخه از اندروید و سخت‌افزار قدرتمند خود، یکی از گزینه‌های ایده‌آل برای علاقه‌مندانِ به فبلت‌هاست. نکسوس P۶ به صفحه نمایش اَمولد با رزولوشن ۲۵۶۰ در ۱۴۴۰ پیکسل مجهز شده و نسخه به‌روزشده پردازنده اسنپدراگون ۸۱۰ در آن به کار رفته است. این دستگاه از سنسور اثر انگشت، دوربین اصلی ۱۲،۳ مگاپیکسلی، خودعکس (سلفی) پنج‌مگاپیکسلی در کنار سه گیگابایت حافظه رم بهره می‌برد.

گلکسی نوت۵ یا وان‌ام۹ پلاس

تنها چند هفته پس از رونمایی رسمی از وان‌ام ۹ اچ‌تی‌سی، این کمپانی نسخه جدیدی از این تلفن را با نام وان‌ام ۹ پلاس معرفی کرد. این محصول کمی از پرچمدار اخیر تایوانی‌ها بزرگ‌تر بوده و طراحی آن بسیار شبیه به وان‌ام ۹ است؛ با این تفاوت که یک سنسور اثر انگشت یکپارچه با دکمه هوم در آن قرار گرفته و به جای یک دوربین، مانند پرچمدار سال گذشته، دو دوربین روی آن قرار گرفته است. اچ‌تی‌سی به این ترکیب Duo Camera می‌گوید. گلکسی نوت۵ اولین گوشی هوشمند سامسونگ با چهار گیگابایت حافظه رم است. این گوشی همچنین به پردازنده پرسرعت هشت‌هسته‌ای، حافظه سریع و صفحه‌نمایش فوق‌العاده باکیفیت مجهز شده است. اما این‌بار سامسونگ علاوه بر سخت‌افزار قدرتمند بر روی طراحی و کیفیت ساخت و همچنین تجربه کاربری نیز تمرکز کرده است و این موارد مهم‌ترین وجه تمایز گلکسی نوت جدید با نوت‌های قبلی است.

لومیا ۹۵۰ ایکس ال یا گلکسی اس۶ اج پلاس

امسال سامسونگ فبلت با لبه‌های خمیده خود را با نام اس۶ اج پلاس معرفی کرد که کاملا مشابه برادر کوچک‌تر خود است و تنها یک گیگابایت رم بیشتر و صفحه‌نمایش بزرگ‌تر ۵،۷ اینچی دارد. سامسونگ با این گوشی بسیار زیبا طرفداران فبلت‌ها را نشانه رفته و قصد جلب نظر طرفداران گوشی با صفحه‌نمایش بزرگ را داشته است. مایکروسافت چندی پیش نسل جدید پرچمداران خود را روانه بازار کرد. نسل جدید گوشی‌های هوشمند این کمپانی شامل لومیا ۹۵۰ و لومیا۹۵۰ ایکس ال می‌شوند. این دو گوشی‌هوشمند مبتنی بر ویندوز ۱۰ نسخه موبایل هستند. مایکروسافت علاوه بر بهره‌گیری از بهترین سخت‌افزار موجود در بازار، دوربین قدرتمندی را نیز روی لومیا ۹۵۰ ایکس ال قرار داده است. اما قابلیت‌های این محصول بیشتر در جنبه نرم‌افزاری نمود پیدا می‌کند و در واقع ویندوز ۱۰ موبایل را باید وجه تمایز آن خواند. لومیا 950XL یک گوشی با ابعاد بزرگ، بدنه پلاستیکی و دوربینی فوق‌العاده است که در بین گوشی‌های ویندوزی برترین محصول موجود در بازار به حساب می‌آید. در سوی دیگر اس S6 Edge+ محصولی متفاوت با گوشی‌های معمول موجود در بازار است. این تلفن با لبه‌های خمیده، بدنه ترکیب فلز و شیشه و ابعاد بزرگی که دارد، با وجود ساختارشکن‌بودن در زمینه طراحی، فروش نسبتا خوبی داشته است.