رویداد

۳۸۰ هزار دلار سرمایه‌گذاری دامنه خلیج‌فارس و پارس

■ **ایسنا:** بحث راه‌اندازی سایت‌هایی با پسوند خلیج‌فارس و پارس مدتی است در فضای سایبری کشور شنیده می‌شود. این موضوع که از سوی سازمان فناوری اطلاعات و مخابرات مطرح شده و پیگیری می‌شود برای عملیاتی شدن حداقل به ۳۸۰ هزار دلار سرمایه‌گذاری نیاز دارد. به گفته علیرضا صالح، رییس مرکز ثبت دامنه‌های آیکان در ایران، آیکان (سازمان جهانی نظارت بر نام‌ها و ارقام اینترنتی) برای ثبت هر دامنه جدید ۱۸۵ هزار دلار هزینه دریافت می‌کند و ثبت‌نام در این سامانه پنج هزار دلار هزینه به دنبال دارد.

پرداخت ۵ درصدی درآمد پیامک به رگولاتوری

■ **فارس:** به گفته مدیرکل مالی همراه اول شرکت ارتباطات سیار با حکم مجتمع قضایی شهید صدر تهران، تا تعیین تکلیف قطعی کمافی‌السابق پنج‌درصد درآمد پیامک را به حساب سازمان تنظیم مقررات و ارتباطات رادیویی واریز می‌کند. فرشاد فتاحی‌نیا در این‌باره بیان کرد: معاون سازمان تنظیم مقررات که گفته بود به نظر می‌رسد همراه اول با مشاهده شرایط و ادله، از به نتیجه رسیدن در محکمه ناامید شده و برای نیمه دوم سال ۹۰، سهم ۲۸/۱درصدی از درآمد پیامک را پرداخته، چنین ادعایی صحت ندارد. وی افزود: همراه اول همان طور که در صفحه ۳۳ از صورت‌های مالی سال ۱۳۹۰ خود به صورت شفاف اعلام کرده سهم سازمان تنظیم مقررات و ارتباطات رادیویی از درآمد پیامک را براساس حکم مجتمع قضایی شهید صدر تهران، تا صدور حکم و تعیین تکلیف قطعی، کمافی‌السابق به صورت پنج‌درصد می‌پردازد اما ۱۸۱۶ میلیارد ریال مابه‌التفاوت پنج‌درصد ملاک عمل همراه اول تا ۲۸/۱ درصد مورد نظر رگولاتوری از درآمد پیامک را، تا صدور رای نهایی دادگاه، به عنوان ذخیره در حساب‌ها منظور کرده است.

رونمایی از طرح کلان «گرید» ملی

■ **مهر:** طرح کلان ملی تورین (گرید) محاسباتی ملی که از سال ۸۸ آغاز شد، روز گذشته با حضور ریاست‌جمهوری رونمایی شد و با راه‌اندازی فاز اول این طرح توان محاسباتی ۵۰برابر می‌شود. هدف از فناوری گرید، یکپارچه کردن منابع پردازشی شامل کامپیوترها، داده‌های خام، آشکارسازها و دستگاه‌های آزمایشگاهی است که از طریق یک شبکه مانند اینترنت به همدیگر متصل می‌شوند. با این اقدام می‌توان منابع محاسباتی دانشگاه‌ها و موسسات یک کشور یا چندین موسسه بین‌المللی را یکپارچه کرد. در فاز اول این طرح کلان ملی در دو دانشگاه کشور اقدام به ایجاد مرکز ابررایانه ملی راه‌اندازی شد و در فاز دوم حداقل در ۱۰ دانشگاه و مرکز علمی دیگر، ابررایانه‌هایی با توان پردازشی کم راه‌اندازی شد.

رد پای آمریکا و اسراییل در انتشار ویروس نفتی

■ **ایسنا:** روزنامه گاردین انگلیس گزارش داد کارشناسان هشدار دادند حمله سایبری ماه گذشته به وزارت نفت ایران و ترمینال اصلی صادرات نفت ایران از سوی پیچیده‌ترین کرم کامپیوتری که تاکنون ساخته شده، بوده است. به نظر می‌رسد این ویروس ابتدا در تعداد کمی از سازمان‌ها و نهادها در ایران، کرانه باختری، لبنان و امارات فرستاده شده است. این مساله به شکل اجتناب‌ناپذیری این شک را برمی‌انگیزد که اسراییل یا آمریکا به شکلی در این ماجرا دست داشته‌اند. تحلیلگرانی که در رمزگشایی این کرم کامپیوتری موسوم به w32 فلامر نقش داشته‌اند، نتوانسته‌اند منشاء این ویروس را شناسایی کنند اما می‌گویند تنها یک تیم حرفه‌ای با چندین ماه کار می‌تواند پشت این قضیه باشد. اورلا کاکس تحلیلگر برجسته شرکت بین‌المللی امنیت کامپیوتری «سیمنتک» در این‌باره می‌گوید: به نظر می‌رسد «w32 فلامر» حتی از استاکس‌نت نیز پیچیده‌تر بوده و یک برنامه جاسوسی بسیار هوشمند و جامع است.

کشف مخرب‌ترین سلاح سایبری در شبکه‌های ایران

فعالیت «شعله آتش» از ۲۰۱۰ آغاز شد

شرق: شعله آتش که با عنوان سلاح سایبری از آن نام برده شده است، پیچیده‌ترین جعبه ابزار فعالیت غیرمجاز سایبری است که تاکنون شناخته شده است و حتی از استاکس نت نیز پیچیده‌تر است. Flamer یا شعله آتش نام سلاح سایبری نهان در شبکه‌های ایران و چند کشور منطقه است که فعالیت مخرب و جمع‌آوری اطلاعات را از سال ۲۰۱۰ میلادی آغاز کرده است. «پایگاه اطلاع‌رسانی امنیت و فضای تبادل اطلاعات»- aftana.ir - می‌نویسد: پیرو انتشار گزارش مرکز ماهر در مورد تحلیل حمله سایبری به وزارت نفت و شناسایی بدافزاری به نام Flamer یا شعله آتش T شرکت کسپراسکای با تایید فعالیت آن، ابعاد جدیدی از آن را مشخص کرده است. این بدافزار ترافیک شبکه را تحلیل می‌کند، از صفحات نمایش عکس می‌گیرد، مکالمات صوتی تحت شبکه را ضبط می‌کند، ضرب کلیدها را ثبت و در نهایت داده‌ها را به مرکز کنترل خودش ارسال می‌کند. نکته قابل توجه در این گزارش این است که ایران بیشترین آسیب را از سال ۲۰۱۰ تاکنون از این بدافزار متحمل شده و احتمالا هدف ۱۸۹ حمله واقع شده است. ضمن آنکه رژیم صهیونیستی با ۹۸ حمله، سودان با ۳۲ حمله، سوریه با ۳۰حمله، لبنان با ۱۸ حمله، عربستان سعودی با ۱۰ حمله و مصر با پنج‌حمله، دیگر هدف‌های این بدافزار بوده‌اند. الکساندر گوستف، از تحلیلگران آزمایشگاه کسپراسکای معتقد است این سلاح سایبری روی هیچ صنعت خاصی نشانه‌روی نشده و صرفا به کار جمع‌آوری داده‌های مهم در هر شبکه‌ای مشغول بوده است و ابزاری با قابلیت جمع‌آوری همه انواع داده‌های حساس بوده است. بنابر اظهارات او آزمایشگاه کسپراسکای پس از اعلام درخواست اتحادیه جهانی مخابرات مبنی بر شناسایی عامل پاک شدن داده‌ها در شبکه‌های چند کشور خاورمیانه وارد عمل شده و اقدام به تهیه و انتشار این گزارش کرده است.

گوستف می‌افزاید: این بدافزار که با نام وایپر (Wiper) نیز شناخته می‌شود حجمی حدود ۲۰ مگابایت دارد و نام دیگر آن Worm. Win32. Flame است. گزارش کسپراسکای تاکید دارد این بدافزار که مجموعه کاملی از همه ابزارهای جاسوسی و جمع‌آوری اطلاعات است، شباهت‌های بسیاری به استاکس نت و دوکو دارد اما به نظر می‌رسد توسط گروه‌های متفاوتی نوشته شده‌اند و احتمالا به موازات یکدیگر توسعه یافته‌اند. کارشناسان کسپراسکای با تاکید بر اینکه این بدافزار در حقیقت یک سلاح سایبری بسیار پیچیده است، از انجام تحقیقات بیشتر روی آن خبر داده‌اند.

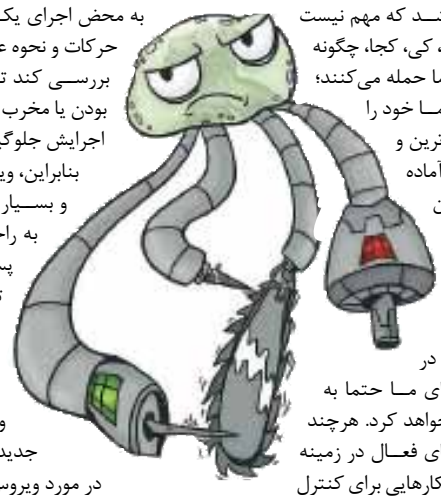
محققان دانشگاه بوداپست هم که نقش مهمی در کشف و شناسایی این بدافزار داشته‌اند، می‌گویند: نتیجه بررسی‌های فنی ما نشان می‌دهد که Flamer (که توسط این گروه sKyWIper نامیده شده)، توسط یک نهاد دولتی نوشته شده که از بودجه فراوان برخوردار بوده است و به انجام فعالیت‌های جنگ سایبری علاقه‌مند است. در این گزارش هم تصریح شده که sKyWIper به طور قطع پیچیده‌ترین بدافزاری است که محققان این دانشگاه تاکنون با آن مواجه شده‌اند و شاید بتوان آن را پیچیده‌ترین بدافزار تاریخ دانست. بی‌بی‌سی نیز در این زمینه به نقل از ویتالی کاملاک رییس شرکت روسی آنتی‌ویروس کسپراسکای می‌نویسد کارشناسان این شرکت موفق به کشف حمله سایبری گسترده موسوم به «فلیم» (شعله) شده‌اند که به طور گسترده از آگوست ۲۰۱۰ مبادرت به جمع‌آوری اطلاعات از برخی کشورهای منطقه مثل ایران، سوریه، سودان، لبنان، مصر و عربستان کرده است. کاملاک مدعی است به رژیم صهیونیستی هم حمله صورت گرفته و به عنوان یکی دیگر از طرف‌هایی که مورد حمله سایبری قرار گرفته وسعت و پیشرفتگی «فلیم» در حدی است که بیانگر این است که این کار توسط یک دولت پشتیبانی می‌شود، اما نمی‌توان مبدأ آن را مشخص کرد. وی همچنین گفته است ۶۰۰ هدف خاص مورد حمله «فلیم» واقع شده‌اند که شامل اطلاعات شخصی افراد، اطلاعات تجاری، اطلاعات موسسات آموزشی و سیستم‌های دولتی می‌شود. با این حال Flamer برای انتشار، خود را روی دستگاه‌های قابل اتصال به پرت‌های یواس‌بی منتقل می‌کند و سپس به سرعت از رایانه‌ای به رایانه دیگر کپی می‌شود. این بدافزار همچنین از یک آسیب‌پذیری قدیمی در ویندوز که مورد سوءاستفاده استاکس نت هم قرار گرفته بود، بهره می‌گیرد. Flamer از چنان قدرتی برخوردار است که حتی رایانه‌های مجهز به سیستم عامل ویندوز ۷ که تمام وصله‌های امنیتی به‌روزرسان روی آنها نصب شده را هم آلوده کرده است. اگر Flamer تشخیص دهد که روی رایانه، نرم‌افزار ضدویروس نصب شده برای جلوگیری از شناسایی خود، از اجرای برخی کدهای مخرب خودداری می‌کند. همین مساله موجب شده تا شناسایی این بدافزار تاکنون دشوار بوده باشد. انتشار از طریق حافظه‌های فلش، انتشار در سطح شبکه، پویش شبکه و جمع‌آوری و ثبت اطلاعات منابع شبکه و رمز عبور سیستم‌های مختلف و همچنین پویش دیسک کامپیوتر آلوده و جست‌وجو برای فایل‌هایی با پسوندها و محتوای مشخص و تهیه تصویر از فعالیت‌های خاص کاربر سیستم آلوده با ذخیره‌سازی تصاویر نمایش داده‌شده روی مانیتور کاربر از جمله قابلیت‌های این ویروس است. در عین حال این ویروس قادر است ذخیره‌سازی صوت دریافتی از طریق میکروفن سیستم در صورت وجود، ارسال اطلاعات ذخیره‌شده به سرورهای کنترل خارج از کشور و شناسایی و از کار انداختن بیش از صد نرم‌افزار آنتی‌ویروس، ضدبدافزار و فایروال را انجام دهد.

وجود هریک از این نشانه‌ها بیانگر آلودگی سیستم به بدافزار flamer است.

ردیف	نوع علائم	آدرس
1	وجود کلید رجیسنری	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Authentication Packages -> mssecmgr.ocx
2	فایلهای اجرایی و تنظیمات آلودگی	windows\system32\mssecmgr.ocx Windows\System32\ccalc32.sys Windows\System32\msglu32.ocx Windows\System32\boot32drv.sys Windows\System32\ntcps32.ocx Windows\System32\advnetcfg.ocx Windows\System32\soapr32.ocx Windows\System32\to961.tmp Windows\ EF_trace.log

امنیت

آیا باید با وایپر خداحافظی کرد؟



شرق: خاطرمان باشد که مهم نیست ویروس‌های رایانه‌ای، کی، کجا، چگونه و با چه شدتی به ما حمله می‌کنند؛ مهم این است که ما خود را برای مقابله با بدترین و خطرناک‌ترین آنها آماده کرده باشیم و این آمادگی را همواره به‌روز نگاه داریم. در این صورت، احتمال ایجاد آلودگی و اختلال در سیستم‌های رایانه‌ای ما حتما به سمت صفر میل خواهد کرد. هرچند برخی از سازمان‌های فعال در زمینه امنیت اطلاعات، راهکارهایی برای کنترل و انسداد حملات وایپر ارایه کرده‌اند، اما این روش‌های پیشنهادی، به هیچ‌وجه موثر نیستند.

نمونه‌ای از روش‌های ارایه‌شده، راهکارهای ببتنی بر محدود کردن دسترسی به فایل - Di kpart یا حذف کامل آن است، اما نکته این است که اضافه کردن این فایل 160 KB به ویروس بسیار ساده بوده و این در حالی است که گزینه‌های بسیار بهتری برای جایگزینی آن در اختیار منتشرکنندگان ویروس است. بهترین و موثرترین راهکار حفاظتی، در نظر گرفتن مرحله اصلی تخریب و جلوگیری از فعالیت این ویروس یا ویروس‌های مشابه در هنگام آغاز عملی حمله‌ای است. بر اساس اطلاعات امنیت فضای تبادل اطلاعات- افتانا- در این رابطه به نظر نمی‌رسد که راهکارهای سنتی ویروس‌یابی یعنی شناسایی ویروس‌ها بر مبنای فایل بروزرسانی (Signature) موثر باشد.

این یک راهکار پساکنترلی محسوب می‌شود و ویروس‌های بسیار جدید معمولا از این سد دفاعی به‌راحتی عبور می‌کنند. به همین منظور برخی از شرکت‌های ضد ویروس راهکارهای امنیتی دیگری دارند که می‌توانند کدهای مخرب را پیش شناسایی کنند. این روش‌های مکمل معمولا بر مبنای رفتارشناسی و حرکت سنجی کدهای اجرایی عمل می‌کنند. نمونه‌ای از قدرتمندترین روش‌های حفاظت پیشگیرانه در مقابله با ویروس‌های اینترنتی که در اختیار شرکت امنیتی پاندا است، به فناوری TruPrevent مشهور است. این تکنولوژی حفاظتی می‌تواند به محض اجرای یک فایل، تمام رفتارها، حرکات و نحوه عملکرد آن را به سرعت بررسی کند تا در صورت مشکوک بودن یا مخرب بودن آن فایل، از ادامه اجرایش جلوگیری شود.

بنابراین، ویروس‌های ثبت نشده و بسیار جدید نیز با این روش به راحتی به دام می‌افتند و پس از قرنطینه شدن و تشخیص قابلیت‌های تخریبی، در پایگاه‌های اطلاعات امنیتی شرکت پاندا و به عنوان یک ویروس جدید ثبت می‌شوند. بله! در مورد ویروس‌های بسیار جدید و بسیار خطرناک که به سرعت در اینترنت منتشر شده یا به صورت هدفدار عمل می‌کنند، متاسفانه روش‌های سنتی شناسایی ویروس‌ها، عملا غیرموثر و بی‌فایده هستند.

تحقیقاتی که توسط تیم فنی شرکت ایمن رایانه روی کد منبع این ویروس W32/ VRBAT انجام شده، نشان می‌دهد فایل‌های اصلی که ویروس تنها با تغییر آنها موفق به انجام فرآیندهای تخریبی خود می‌شود، با عنوان Ntldr و Bootmgr فایل‌های سیستمی بسیار حیاتی هستند که باید دسترسی به آنها تحت کنترل کامل مدیر شبکه باشد. با استفاده از روش‌های پیشگیرانه حفاظتی مانند - Panda TruPr vent، نه تنها می‌توانیم دستورالعمل‌های جدید و دلخواه حفاظتی برای انسداد دسترسی به این دو فایل حساس سیستمی تعریف کنیم، بلکه می‌توانیم این ماژول‌های جدید حفاظتی را روی تمام سرورها و رایانه‌های سازمانی اعمال کنیم. در این حالت ویروس‌هایی که با تغییر فایل‌های Ntldr و Bootmgr فعال می‌شوند، در عمل قادر به تخریب رایانه شما نخواهند بود. همچنین راهکارهای عمومی امنیت اطلاعات مانند امن نگاه داشتن پورت‌های یو اس بی با استفاده از برنامه Panda USBVaccine، نصب اصلاحیه‌های امنیتی سیستم عامل روی تمام ایستگاه‌های کاری شبکه و نیز تعریف صحیح پیکربندی امنیت شبکه می‌توانند در شناسایی و کنترل سریع و پیشگیرانه حملات و ویروس‌های رایانه‌ای مفید باشند.

بازیکده

نگاه‌ها به ۱۱ بازیکن

مجید نوردوست: مدتی پیش بازی PES 2013 معرفی شد و حالا نوبت به EA رسیده که با بازی محبوبش که همان FIFA 13 باشد، وارد رقابت این فصل از دنیای فوتبال شود. تهیه‌کننده سری بازی‌های FIFA آقای دیوید روتر (David Rutter) بازی FIFA 13 را در نمایشی در لندن معرفی و اولین اطلاعات و تصاویر این بازی را منتشر کرد. برخلاف انتظارها و پیش‌بینی‌ها که حاکی از آن بودند که FIFA 13 در مقایسه با FIFA 12 تغییر زیادی نخواهد داشت، اما آقای روتر اعلام کرد که بازی FIFA 13 دارای پنج تغییر بسیار اساسی و مهم نسبت به نسخه قبلی است. اولین چیزی که در FIFA 13 متوجه آن می‌شوید، کنترل واقعی‌تر توپی است که در اختیار بازیکنان قرار می‌گیرد. در این بازی کنترل توپی که برای بازیکنان ارسال می‌شود، سخت‌تر شده است. در واقع آن بازیکنی که توپ را برایش ارسال کرده‌اید، باید مهارت لازم برای دریافت توپ را داشته باشد. این موضوع به قدرت و سرعت توپ و ارتفاعی که توپ به هوا بلند می‌شود هم بستگی دارد. یکی دیگر از قابلیت‌هایی که در این نسخه بهبود پیدا کرده، Impact Engine یا موتور برخوردی است که از نسخه FIFA 12 به این سری از بازی‌ها اضافه شده است. Impact Engine باعث به وجود آمدن برخوردهای بسیار واقعی‌تر و نمایش‌های فیزیکی بهتری در FIFA 12 شد، اما برخی اوقات بازیکنان صحنه‌های اغراق‌شده زیادی را مشاهده می‌کردند. در FIFA 13 دیگر این‌گونه انیمیشن‌ها را مشاهده نمی‌کنید. در FIFA 12 با تغییر جهت دادن می‌توانستید بازیکنان حریف را دریبل بزنید. اما این امکان در FIFA 13 دیگر وجود ندارد و برای دریبل کردن باید از مهارت زیادی برخوردار باشید. یک سیستم جدید برای ضربه‌های ایستگاهی بازی طراحی شده است. اکنون سه بازیکن مختلف می‌توانند در زمان ضربه‌های ایستگاهی پشت توپ قرار بگیرند. همچنین می‌توانید بازیکنانی از تیم خود را هم در خط دفاعی حریف قرار دهید تا برای بازیکنان خط دفاعی دردسرساز شوند. یکی از قسمت‌های جالب این است که در زمان ضربه‌های کاشته می‌توانید حرکت‌های نمایشی و گول‌زننده از خود اجرا کنید تا بازیکنان را بر سر تشخیص مسیر توپ به اشتباه بیندازید. هوش مصنوعی بازی در زمان دفاع آنقدر خوب بوده که تیم سازنده تغییراتی را در آن ایجاد نکرده، اما هوش مصنوعی در زمان حمله تغییراتی به همراه داشته تا بتواند به چالش خوبی برای مدافعان تبدیل شود. CPU بازیکنان بدون توپ را به شکل بسیار بهتری کنترل می‌کند و کاری می‌کند تا بازیکنی که توپ را در اختیار دارد از گزینه‌های بهتری برای پاس دادن و انجام کارهای مختلف برخوردار باشد. همچنین بازیکنان به شکل بسیار هوشمندانه‌تری حمله و بسیار خوب می‌توانند خود را از آفساید خارج کنند. آنها منتظر ارسال توپ می‌مانند و پس از ارسال آن، به سمت دروازه حریف حرکت می‌کنند. همچنین عملکرد داورها هم در این بازی بهتر خواهد شد تا فضای فوتبالی بهتری در بازی به وجود بیاید. آقای روتر به این مساله اشاره کرد که آنها از یک نرم‌افزار Dimensional Imaging در بازی استفاده کرده‌اند که باعث می‌شود گرافیک FIFA 13 بهتر از نسخه‌های قبلی باشد. در FIFA 13 می‌توانیم این انتظار را داشته باشیم که بازیکنان معروف دنیای فوتبال به شکل واقعی‌تری در بازی طراحی شده باشند. دلیل آن هم همین Dimensional Imaging جدیدی است که در بازی به کار رفته است. روتر به این موضوع اشاره می‌کند که در نسخه‌های قبلی به دلیل تکنولوژی‌ای که برای آن بازی‌ها استفاده می‌شد، فقط می‌شد تعداد مشخصی از بازیکنان محبوب را به صورت واقعی طراحی کرد. اما با استفاده از تکنولوژی جدید به‌کاررفته در FIFA 13 آنها می‌توانند بازیکنان بیشتری را به شکل واقعی طراحی کنند. آقای مایک هریسون (Mike Harrison) کارگردان بخش Mo-Cap بازی‌های EA می‌گوید: «ما از چند سال پیش متوجه شدیم که باید کیفیت طراحی صورت بازیکنان را بالا ببریم، مخصوصا بازیکنانی که در تیم‌های بسیار محبوب و بزرگ بازی می‌کنند. ما با نرم‌افزار Dimensional Imaging به شکل بسیار خوبی کار کردیم که به ما این امکان را می‌دهد تا در خلق مدل‌های 3D از دقت بیشتری برخوردار باشیم و بتوانیم صورت‌ها را به شکل بسیار بهتری Capture کنیم. نتیجه کار هم بسیار بهتر از چیزی بود که ما انتظار آن را داشتیم.» ققای کالین آرکهارت (Colin Urquhart) رییس - D mensional Imaging نیز به این موضوع اشاره می‌کند که: «این موضوع بسیار مهم بود که کیفیت گرافیکی بازی بسیار به حرکات واقعی یک انسان شباهت داشته باشد تا بتوان به وسیله آن شخصیت‌های مجازی بهتری خلق کرد، اما روش‌های سنتی باعث می‌شدند که این کار زمان بیشتری بگیرد. EA از اولین بازی‌سازانی بود که تشخیص داد باید دست به چنین کاری بزند و باید سیستم Capture خودش را ارتقا دهد. ما از FIFA 10 با آنها کار می‌کردیم و سرانجام موفق شدیم سیستم Dimensional Imaging را برای FIFA 13 خلق کنیم؛ فناوری‌ای که کار کردن با آن بسیار راحت‌تر از فناوری‌های مشابه است و امکانات بسیار بیشتری هم در بر دارد.» بازی FIFA 13 به احتمال بسیار زیاد در پاییز امسال راهی بازار خواهد شد.

گذرگاه

موانع توسعه خدمات باندوسیع

سمیه تاجیک*

■ گرچه حدود هشت سال از ایجاد اولین خط DSL و اعطای پروانه ارایه خدمات انتقال داده‌ها (PAP) می‌گذرد، اما ضریب نفوذ ارتباطات باندوسیع کشور تا پایان سال ۲۰۱۱ تنها دو درصد بوده است. البته نتایج نظرسنجی‌های داخلی نشان می‌دهد که علاقه مردم در ایران به سرویس‌های اینترنتی بسیار بالاست و در نتیجه ضرورت توسعه باندوسیع در کشور بیش از پیش برجسته و مهم می‌شود. از طرف دیگر، امروزه توسعه باندوسیع در اکثر کشورهای پیشرفته و در حال توسعه به عنوان یکی از مهم‌ترین زیربناهای رشد خدمات ارزش افزوده الکترونیکی و ارتباطی در همه بخش‌های اقتصادی، فرهنگی و اجتماعی کشور معرفی و تاکید شده است. از این رو، در ششم خرداد سال‌جاری، نشست هم‌اندیشی «بررسی راهکارها و موانع توسعه خدمات باندوسیع در کشور» با حضور تنی چند از مسوولان و مدیران ارشد شرکت‌های ارایه‌دهنده خدمات باندوسیع ثابت برگزار شد. در این نشست صیدی، رییس مرکز توسعه فناوری اطلاعات شرکت مخابرات ایران بیان کرد: مطالعات ما نشان می‌دهد کشورهای مختلف اروپایی، آسیایی و چند کشور همسایه نظیر ترکیه از سال ۲۰۰۰، توسعه باندوسیع را به صورت جدی شروع کرده‌اند. البته ایران نیز حدود سال ۲۰۰۳، فعالیت در این حوزه را با تدوین آیین‌نامه‌های مربوطه و اعطای مجوز آغاز کرد. با این حال او نیز بر این باور است که موضوع اصلی در این است که متاسفانه برعکس روند مناطق توسعه‌یافته و در حال توسعه، پیش رفته‌ایم. کشورهای در حال توسعه، اپراتورهای غالب را از ارایه خدمات باندوسیع منع نکردند، در حالی که منع ورود اپراتور غالب به این حوزه، فقط در کشورمان رخ داده است. البته رییس مرکز توسعه فناوری اطلاعات شرکت مخابرات ایران رویکرد کشور در حوزه تلفن همراه را مشابه کشورهای دیگر دانسته و معتقد است اپراتور غالب توانست در حوزه تلفن همراه ورود پیدا کند و در نتیجه، از نظر کمی و کیفی رشد قابل توجهی را تجربه کردیم. در مقابل خادمی مسوول کمیسیون اینترنت نظام صنفی بیان می‌کند از نقطه نظر رگولاتوری نیز باید بدانیم که بسیاری از کشورها پس از ما صاحب رگولاتوری شده‌اند. البته در رگولاتوری ما نیز، باید نگاه فرابخشی حاکم شود و از سوی دیگر قدرت رگولاتوری نیز افزایش یابد. او با اشاره به نقاط ضعف رگولاتوری کشور به تعرفه‌های خدماتی در ایران و دیگر کشورها پرداخته و می‌گوید: به طور مثال، قیمت یک STM1 از حدود ۱۲ هزار دلار در چند سال پیش به حدود چهار هزاردلار در حال حاضر کاهش یافته است، این در حالی است که اصلا تغییری در تعرفه‌ها صورت نگرفته است. کریمی نیز هزینه انتقال را غیرمنطقی می‌داند و بر این باور است که در حوزه انتقال دیتا، قیمت‌ها خیلی غیرمنطقی است و هزینه ارسال یک بسته اطلاعات در بین استان‌ها حتی با هزینه یک‌بار انتقال دور کره زمین برابری می‌کند. این موضوع از دلایل بالا بودن تعرفه خدمات DSL محسوب می‌شود. اصفهانی، مدیرعامل شرکت ارتباطات مبین‌نت نیز بر این عقیده است اگر مشخص شود که باندوسیع یک نیاز جامعه است، آنگاه که با عزمی ملی می‌توانیم همه مشکلات آن را حل کنیم. بنا بر اظهارات او نگاه‌ها در سیاستگذاری فناوری‌محور بوده و این در حالی است که باید سرویس‌محور باشد. به طور مثال به اپراتور، پروانه WiMAX می‌دهند. این در حالی است که با توجه به افول این فناوری، تولید تجهیزات آن تا چند سال آینده متوقف خواهد شد و این به آن معناست که اگر در پروانه فعالیت تجدید نظر نشود، اپراتورهای وایمکس از بین خواهند رفت. نکته قابل توجه در این میان اظهارات مسوولان دولتی است که پایه‌های سیاستگذاری در این حوزه را اشتباه می‌دانند. پوررنگ‌نیا، عضو هیات مدیره شرکت ارتباطات زیرساخت می‌گوید: ما تقریبا در بحث پهنای باند بین‌الملل مشکلی نداریم ولی مشکل اصلی را می‌توان در گسترش پهنای باند داخلی دانست اما متاسفانه از ابتدا سیاستگذاری مناسبی در نظر گرفته نشده و کل سیم مسی را در اختیار شرکت مخابرات قرار داده‌ایم و ایراد اصلی اینجاست. شاهی، معاون بهره‌برداری و مدیریت شبکه شرکت ارتباطات زیرساخت نیز معتقد است نحوه نگاه به بحث دیتا نگاه درستی نیست. یکی از آفت‌هایی که در این زمینه وجود دارد این است که بازیگرانی که به این بحث ورود پیدا می‌کنند، بیشتر به دنبال منافع مالی آن هستند و همین که فعالیت آنها به سوددهی زودهنگام برسد آنان را قانع می‌کند. با این حال در توسعه باندوسیع نباید به یک موضوع بیشتر و به یک موضوع کمتر پرداخت. بنا بر اظهارات گوران، همه بخش‌های زنجیره ارزش در یک اولویت قرار دارند و باید به توسعه باندوسیع در کنار ارایه‌دهنده سرویس و در کنار ارایه‌دهنده محتوا و به صورت یکجا با هم نگاه کرد و همه را به صورت موازی هم پیش برد. گرچه در این میان انحصار، عامل عدم توسعه باندوسیع در کشور است اما تاجمیری، نیز بر این باور است که مبنای کل اختلافات بین PAPها و مخابرات منابعی بوده است که به صورت انحصاری در اختیار مخابرات قرار دارد و این شرکت مالک اصلی آن به شمار می‌رود و این امر را می‌توان یکی از عوامل عدم توسعه باندوسیع در ایران تلقی کرد. از سوی دیگر PAPها به جز تجهیزات DSLAM و router، نمی‌توانند تجهیزات دیگری را برای ارایه خدمات، وارد مراکز مخابراتی کنند و عملا نمی‌توانند وارد بازار ارایه IPTV شوند.

* گروه تحلیلی طیف