خبر

بهره‌برداری رسمی از وایمکس سراسری

مدیرعامل اپراتور وایمکس مبین‌نت از بهره‌برداری رسمی شبکه وایمکس سراسری از مردادماه امسال خبر داد. به گزارش شرق، محمدتقی خاکی با اعلام این خبر گفت: «در عین حال تا پایان سال ۹۰، ۳۷۹ شهر زیر پوشش شبکه اینترنت وایمکس قرار می‌گیرد. اظهارات این مقام مسوول برنده مزایده وایمکس در حالی بیان می‌شود که این اپراتور موظف بود ۹ماه پس از اعطای پروانه، فعالیت خود را آغاز و اقدام به ارائه سرویس به مشترکان کند که این امر محقق نشد. در عین حال بهمن‌ماه سال گذشته مسوولان این شرکت در یک نشست خبری بیان کردند تا پایان خردادماه شبکه سراسری وایمکس به بهره‌برداری کامل خواهد رسید که با وجود گذشت هفتم ماه مدیرعامل جدید این شرکت بیان کرد به دلیل پاره‌ای مسائل که از حیطه فعالیتی آنها خارج بود، نتوانستند به این مهم دست یابند. خاکی در ادامه با اشاره به تاخیرهای این اپراتور و احتمال جریمه شدن از سوی سازمان تنظیم مقررات ادامه داد: «در زمان تاخیر، رگولاتوری جریمه‌هایی را برای اپراتورها در نظر می‌گیرد که اگر مشمول جریمه شویم و در این زمینه تصمیم گرفته شود، باید تابع باشیم.»

جلوگیری از فروش تجهیزات مخابراتی قاچاق

رئیس مرکز امور بین‌الملل سازمان تنظیم مقررات و ارتباطات رادیویی بر لزوم جلوگیری از فروش تجهیزات مخابراتی قاچاق و غیراستاندارد تاکید کرد. به گزارش ایسنا، صادق عباسی در این باره گفت: «یکی از مشکلات موجود در کشور تنوع بیش از حد مدل‌های تجهیزات مخابراتی در بازار است اما اگر واردکنندگان دقت کرده و فقط مدل‌های تاییدشده را به کشور وارد کنند، از مشکلات بعدی ناشی از عدم تایید، پیشگیری و اجازه ورود ساده‌تر دریافت می‌شود.» وی ادامه داد: «با توجه به اینکه همه تجهیزات مخابراتی به هم مربوطند، بنابراین لازم است همه از استانداردهای خاصی تبعیت کنند تا بتوانند با هم کار کنند.» وی افزود: «با توجه به اینکه این نوع تجهیزات از مجاری قانونی وارد نمی‌شوند و به‌طور طبیعی به آنها دسترسی وجود ندارد، در صورت واصل شدن شکایت یا کشف موردی در نظارت‌های معمول سازمان، این موضوع بررسی و درصورت عدم تطابق با استانداردها و ضوابط، از فروش و استفاده آنها جلوگیری می‌شود.»

دریافت ۱۷۱۹ میلیارد تومانی رگولاتوری

مدیر کل دفتر برنامه و بودجه سازمان تنظیم مقررات از دریافت ۱۷۱۹ میلیارد تومان از اپراتورها و واریز به خزانه دولت در سال جاری خبر داد. به گزارش ایسنا، محمد محرابی با اعلام این خبر گفت: «سازمان تنظیم مقررات و ارتباطات رادیویی باید طبق تعهدی که در سال ۸۹ دارد، مبلغ ۱۷۱۹ میلیارد تومان از اپراتورها گرفته و به خزانه دولت واریز کند.» وی ادامه داد:«این مبلغ از اپراتورهای اول و دوم و بقیه اپراتورهای SAP،PAP و ISPها دریافت می‌شود اما بخش عمده آن، یعنی ۹۰ درصد پول، در قالب اپراتور اول و دوم است که حدود ۱۳۰۰ میلیارد تومان آن در حوزه اپراتورها و حق‌السهم آنها است.» به گفته وی خزانه بر اساس پولی که می‌گیرد، سهم بخش فناوری اطلاعات و ارتباطات یعنی وزارت ارتباطات، پست، فناوری اطلاعات، زیرساخت، سازمان تنظیم مقررات و سازمان فضایی را از این محل پرداخت می‌کند. به گفته وی سال گذشته حدود ۱۰۴۸ میلیارد تومان تعهد رگولاتوری بود که آن را وصول کرده و به حساب خزانه واریز شد.

واگذاری ۴۴ هزار پورت اینترنت پرسرعت

به گفته مدیر روابط عمومی مخابرات استان تهران ۴۴ هزار و۲۹۴ پورت اینترنت پرسرعت تا پایان تیرماه در تهران واگذار شد.
محمد خجسته‌نیا با بیان مطلب فوق افزود: «آمار واگذاری ADSL در استان تهران تا پایان خردادماه ۴۱ هزار و ۵۰۳ عدد بود.» وی ادامه داد: «مخابرات استان تهران از نیمه دوم اسفندماه گذشته، واگذاری ۸۰ هزار پورت را آغاز کرد اما پیش از آن به دلیل منع قانونی، شرکت‌های مخابرات استانی برای ارائه اینترنت پرسرعت، در سال‌های پیش از این تنها ۱۶ هزار و ۱۳۶ عدد را به مشاغل خاص ارائه داده است.» وی گفت: «در منطقه ۲، ۱۴ هزار و ۸۲۳، منطقه ۳، ۷۳۱، منطقه ۴، هزار و ۳۶۴، منطقه ۵، ۲۳۸، منطقه ۶، هزار و ۵۴۵، منطقه ۷، هزار و ۴۵۴ و در منطقه ۸، پنج هزار و ۲۰۲ و در مجموع ۲۵ هزار و ۳۶۷ پورت واگذار شده، که این آمار تا پایان خردادماه گذشته را شامل می‌شود.»

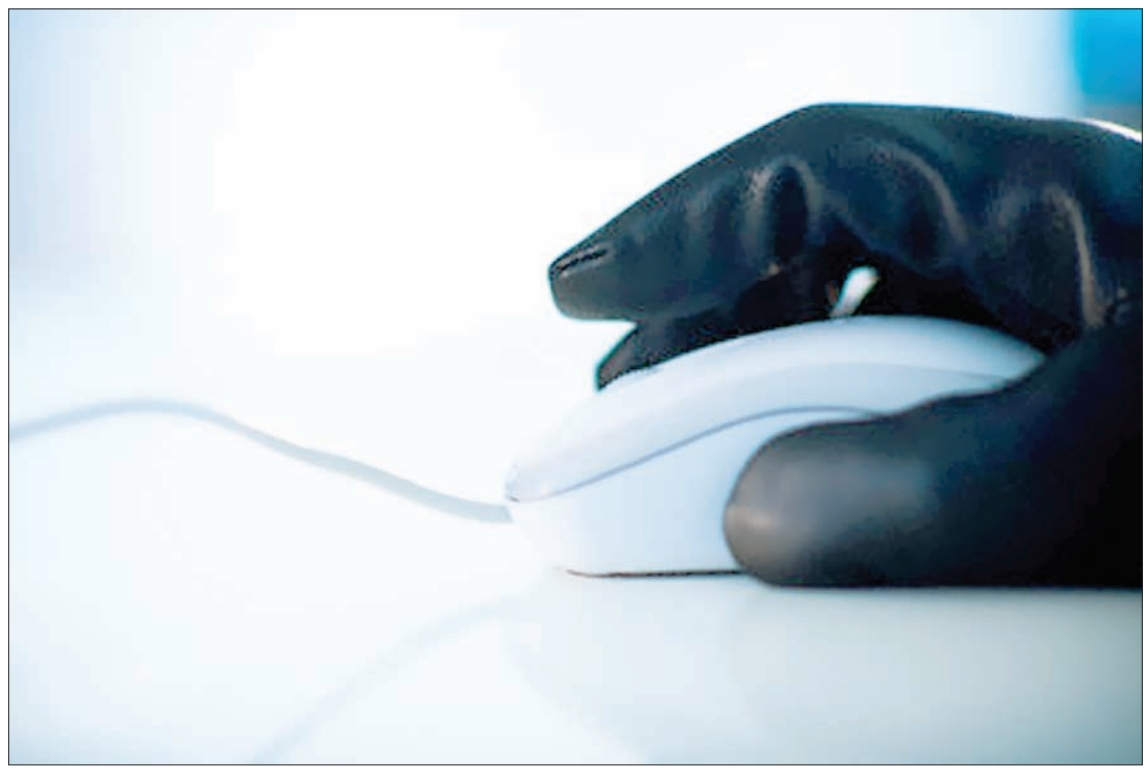
هشدار مجدد به شرکت‌های آی‌تی

موسسه تحقیقاتی گارتنر خطاب به شرکت‌های آی‌تی گزارشی منتشر کرده و اخطار داده شرایط فعلی ممکن است پایدار نباشند و احتمال آغاز دوره‌ای تازه از رکود اقتصادی کماکان وجود دارد.
به گزارش خبرگزاری‌ها به نقل از اینفو ورلد، در بخشی از این گزارش آمده است: در سال ۲۰۰۸ اکثر مدیران شرکت‌های آی‌تی برای مقابله با بحران اقتصادی جهانی آماده نبودند لذا نمی‌توان آنها را ملامت کرد. اما این بار از ماه‌ها قبل هشدارهای لازم به آنها داده شده است و باید توجه داشت که ظرف ۱۲ تا ۱۸ ماه آینده احتمال وقوع یک بحران جدید اقتصادی کاملاً جدی است. به اعتقاد گارتنر مدیران باید فهرستی از طرح‌های غیرضروری خود که اجرای آنها قابل به تعویق انداختن است، آماده کنند تا در صورت وقوع هرگونه مشکل با توقف آنها از به بار آمدن خسارات مالی جدی جلوگیری به عمل آورند. گارتنر که چندی قبل رشد صرف بودجه در حوزه آی‌تی را در سال جاری ۵/۳ درصد پیش‌بینی کرده بود این رقم را به ۳/۹ درصد کاهش داد و بحران اقتصادی اروپا را در این مساله تاثیرگذار دانست.

رایانه‌های ایران مورد هجوم شدید کرم Stuxnet قرار گرفت

سرقت اطلاعات سیستم‌های کنترل صنعتی ایران

حامد شفیعی



رایانه‌های ایران مورد هجوم شدید کرم خطرناک رایانه‌ای به نام Stuxnet قرار گرفته‌اند که تلاش می‌کند اطلاعات سیستم‌های کنترل صنعتی را به سرقت ببرد. ایران بیش از دیگر کشورها به کرم رایانه‌ای خطرناک SCADA موسوم به Stuxnet که هدف آن سرقت اطلاعات از سیستم‌های کنترل صنعتی بوده، آلوده شده است؛ خبری که در اوایل هفته به سرعت در رسانه‌های داخلی انتشار یافته و به دنبال آن سایت‌های خارجی نیز به ارائه گزارش‌های تکمیلی از نحوه شناسایی و مقابله شرکت‌های امنیتی با آن پرداختند. آنچه در این مورد حائز اهمیت بوده، این است که این کرم رایانه‌ها در کشورهای منطقه فعال شده و به غیر از ایران کشورهای هندوستان و اندونزی نیز گرفتار این مساله شده‌اند، اما با این وجود ایران به عنوان آلوده‌ترین کشور به این کرم شناخته شد. نکته قابل توجه این است که این کرم توسط رایانه یک کاربر ایرانی انتشار یافته است؛ با این حال شرکت‌های امنیتی کشوری مانند روسیه را عامل انتشار این ویروس دانسته و بیان کرده‌اند نسبت به این قضیه مشکوک هستند. با این وجود تاکنون مسوولان روس هیچ واکنشی به این مساله نشان نداده‌اند. برای نخستین بار ماه گذشته یک شرکت تولیدکننده نرم‌افزارهای امنیتی واقع در کشور بلاروس به نام VirusBlockAda هنگام گشت‌زنی در اینترنت توانست این کرم را در رایانه یکی از مشتریان ایرانی خود شناسایی کند؛ درعین حال شرکت امنیتی سیمانتک اعلام کرده است، سیستم‌های ایرانی هدف اصلی کرم SCADA وحملات بدافزار Stuxnet بوده است. بر اساس آخرین اطلاعات منتشرشده از سوی این شرکت امنیتی امریکایی، حدود ۶۰ درصد تمام رایانه‌های دنیا که به این کرم آلوده شده‌اند در کشور ایران قرار دارند. دو شرکت امنیتی امریکایی و بلاروسی در حال حاضر به دنبال شناسایی عامل و منشاء این کرم هستند، البته آنها گمان می‌کنند منشاء آن نزدیک کشور ایران است. اعلام رسمی خبر انتشار این کرم رایانه‌ای در حالی از سوی رسانه‌ها صورت می‌گیرد که در ایران دو مرکز به نام‌های «آپا» و «ماهر» با هدف مقابله با تهدیدهای رایانه‌ای در کشور ایجاد شده است، اما مسوولان هر دو طرح از وجود چنین رویدادی اظهار بی‌اطلاعی می‌کنند. این کرم به دنبال سیستم مدیریتی SCADA زیمنس که معمولاً در کارخانه‌های بزرگ تولیدی و صنعتی مورد استفاده قرار می‌گیرد، بوده و تلاش می‌کند اسرار صنعتی رایانه‌های این کارخانه‌ها را بر روی اینترنت بارگذاری (Upload) کند. از این رو وجود این کرم خطر مهمی برای امنیت صنعت کشور تلقی می‌شود. شرکت زیمنس آلمان که تهیه‌کننده این نرم‌افزار مدیریتی برای کارخانه‌ها و صنایع برای کشورها از جلمه ایران است از اعلام تعداد مشتریان خود در ایران سر باز زده و تنها اعلام کرد که دو شرکت آلمانی به واسطه این کرم توسط رایانه‌هایی در ایران آلوده شده‌اند. این شرکت بر روی وب‌سایت خود آنتی‌ویروسی را به صورت رایگان برای مقابله قرار داد.

اعلام رسمی خبر انتشار این کرم رایانه‌ای در حالی از سوی رسانه‌ها صورت می‌گیرد که در ایران دو مرکز به نام‌های «آپا» و «ماهر» با هدف مقابله با تهدیدهای رایانه‌ای در کشور ایجاد شده است. با این وجود دو مرکز امداد رایانه‌ای به نظر می‌رسد نتوانسته‌اند از یکی از بزرگ‌ترین آزمون‌ها که می‌توانست فرصتی برای عرض اندام باشد، سربلند بیرون بیایند.

آپا و ماهر غافلگیر شدند

به دنبال انتشار این کرم، طی ارتباط تلفنی با مسوولان طرح‌های «آپا» و «ماهر» آنها از وجود چنین مساله‌ای اظهار بی‌اطلاعی کردند. از طرفی سجادی مجری پروژه «آپا» در مرکز تحقیقات مخابرات ایران بیان کرد که این وظیفه شرکت فناوری اطلاعات و مجری طرح «ماهر» بوده و در حیطه وظایف کاری طرح «آپا» نیست. در همین حال مسوولان شرکت فناوری اطلاعات از ارائه اطلاعات در این زمینه خودداری کردند به نحوی که طی تماس تلفنی با مجری طرح «ماهر»، او با این توجیه که برای نخستین بار است که با وی تلفنی ارتباط برقرار می‌کنیم، از گفت‌وگو با خبرنگار شرق خودداری کرده و در این زمینه خواستار هماهنگی با روابط عمومی این شرکت شد؛ روابط عمومی شرکت نیز که در مرخصی بود، گرچه درخواست ما را پذیرفت و با وجود دریافت پرسش‌های ما در این زمینه وعده هماهنگی داد اما هیچ گونه هماهنگی‌ای در این زمینه صورت نگرفت تا پیگیری شرق در این زمینه بی‌نتیجه بماند. آپا با موضوع آگاهی‌رسانی، پشتیبانی و امداد حوادث رایانه‌ای که مسوولان وزارت ارتباطات و فناوری اطلاعات از آن به عنوان اورژانس رایانه‌ای ایران یاد می‌کنند، آذرماه سال ۸۷ راه‌اندازی شد. فعالیت‌های مرتبط با شناسایی تهدیدات رایانه‌ای، رصد و کشف آسیب‌پذیری‌های موجود در انواع فناوری‌های اطلاعاتی و ارتباطی، رسیدگی و کمک به سازمان‌های مختلف هنگام بروز حوادث ناشی از حملات رایانه‌ای از جمله اهداف و وظایف این طرح است. در همین حال ماهر - مرکز امداد و هماهنگی رایانه‌ای-پروژه موازی با این طرح در شرکت فناوری اطلاعات راه‌اندازی شده بود که همان وظایف طرح آپا را بر عهده دارد. با وجود این دو مرکز امداد رایانه‌ای به نظر می‌رسد نتوانسته‌اند از یکی از بزرگ‌ترین آزمون‌ها که می‌توانست فرصتی برای عرض اندام باشد، سربلند بیرون بیایند؛ کرم Stuxnet که به دنبال سیستم‌های مدیریت SCADA که متعلق به زیمنس بوده و در کارخانه‌های بزرگ مورد استفاده قرار می‌گیرد، توانسته با آلوده کردن رایانه‌های ایرانی، ایران را در رتبه نخست کشورهای آلوده به این کرم قرار دهد. این کرم بعد از دسترسی به رازهای صنعتی آنها را بر روی اینترنت قرار می‌دهد. SCADA مخفف Supervisory Control And Data Acquisition به معنی کنترل نظارت مدیریتی و دریافت داده‌ها است. همان گونه که از نام این نرم‌افزار مشخص است، اسکادا به یک سیستم کنترل گسترده اشاره داد. این سیستم برای نظارت یا کنترل پروسس‌های شیمیایی یا حمل و نقلی در سیستم‌هایی نظیر تامین آب شهری، کنترل نیروی برق، انتقال و توزیع آن، لوله‌های نفت و گاز و بسیاری پروسس‌های توزیع‌شده دیگر استفاده می‌شود. از این رو اطلاعات مهم و محرمانه‌ای در این سیستم وجود دارد که برای برخی نهادها و شرکت‌ها حائز اهمیت بوده و ممکن است کشورهای رقیب برای شکست حریفان و رقبای خود دست به تخریب این سیستم بزنند. به همین خاطر برخی کارشناسان یکی از دلایل انتشار این کرم را در رایانه‌های کشورهای آسیایی به ویژه ایران به دست آوردن اطلاعات محرمانه و انتشار عمومی آن برای تضعیف می‌دانند. بنابر اظهارات کارشناسان این کرم به چند دلیل قابل توجه است؛ این کرم برای انتشار خود از یک ضعف امنیتی جالب و البته ناشناخته استفاده می‌کند. در عین حال روش اصلی انتشار آن از طریق آلوده کردن فلش‌دیسک‌های متصل شده به سیستم است. البته این کرم از روش‌های دیگری نیز استفاده می‌کند.

جاسوسی کوچک اما سارقی بزرگ

کرم Stuxnet از نام کاربری و کلمه عبوری که در نرم‌افزار زیمنس به صورت hard-coded وجود دارد، سوءاستفاده می‌کند. همچنین این بدافزار با جعل گواهینامه‌های معتبر برای اعتباردهی به خود استفاده می‌کند تا بتواند بر روی سیستم‌های رایانه‌ای بنشیند. شرکت‌های امنیتی این کرم را یک جاسوس شرکتی یا دولتی معرفی کرده‌اند که تنها قصد آن سرقت اطلاعات - نه صدمه زدن به رایانه - است و به محض فعال شدن شروع به ربودن اطلاعات موجود در پایگاه داده‌ها می‌کند. در همین راستا شرکت زیمنس به کاربران خود در مورد تغییر کلمات رمز عبور تعبیه‌شده در کد هشدار داد. این اقدام زیمنس به دنبال انتشار اخباری مبنی بر آلودگی سیستم‌های رایانه‌ای زیرساخت‌های حیاتی در ایران و هند که دارای نرم‌افزارهای این شرکت هستند، صورت گرفت. آنها اعلام کرده‌اند که به زودی یک راهنمای امنیتی را برای کاربران منتشر خواهند کرد. گرچه شرکت امنیتی VirusBlockAda در بلاروس نخستین نمونه این کرم را هنگام جست وجو در اینترنت و در رایانه مشتریان ایرانی خود یافته است اما مسوولان شرکت سیمانتک در مورد اینکه چرا اکثر آلودگی‌ها در ایران و کشورهای هند و اندونزی گزارش شده است، اطلاع دقیقی ندارند و تنها به این نکته بسنده کرده‌اند که نویسنده کرم، شرکت‌ها یا کارخانه‌های محدوده جغرافیایی ایران، هند و اندونزی را هدف قرار داده است. به گفته مدیران شرکت سیمانتک یکی از دلایل گسترش این کرم در رایانه‌های ایرانی کمبود آنتی‌ویروس‌های مناسب بر روی سیستم‌های آنان است. شرکت سیمانتک که یک شرکت امریکایی است و در ایران تنها عامل پخش داشته و به دلایل تحریم نمایندگی ندارد، بیان کرده است، می‌تواند دقیقاً مشخص کند که چه شرکت‌ها و سازمان‌هایی آلوده این کرم شده‌اند. بنابر اعلام مسوولان این شرکت رایانه‌های آلوده شده به سازمان‌های زیادی تعلق داشتند که از نرم‌افزار و سیستم‌های اسکادا استفاده می‌کردند؛ مساله‌ای که به روشنی مورد هدف حمله هکرها بوده است، یعنی نرم‌افزار SCADA زیمنس. کرم Stuxnet توسط ابزارهای USBدار انتقال پیدا می‌کند؛ زمانی که ابزاری آلوده به رایانه متصل می‌شود، کدهای این کرم به جست‌وجوی سیستم‌های زیمنس گشته و خود را بر روی هر ابزار USBدار دیگری که بیابد، کپی خواهد کرد. با این حال سیمانتک اعلام کرده کاربران، شرکت‌ها و سازمان‌ها با خرید نرم‌افزار این شرکت می‌توانند این کرم را پاک کنند.

نگاه آی‌تی

از فیس‌بوک تا «دات ایران»

آرام حامدی

خلاف عادت هر هفته ستون نگاه آی‌تی که در ابتدا با رویدادهای داخلی آغاز می‌شد، این بار ستون این هفته با یک خبر خارجی که توانست در این هفته سهم قابل توجهی از اخبار رسانه‌های داخلی و حتی خارجی را به خود اختصاص دهد و گزارش‌هایی در مورد آن نوشته شود، شروع می‌شود. رسانه‌ها در این هفته اعلام کردند با عبور کاربران فیس‌بوک از مرز ۵۰۰ میلیون نفر در سرتاسر جهان، این شبکه اجتماعی اینترنتی را می‌توان پس از چین و هند سومین کشور پرجمعیت دنیا دانست؛ شبکه اجتماعی‌ای که از شش سال پیش وارد دنیای مجازی شده و احتمال اینکه در آینده کاربران این شبکه اجتماعی مجازی به یک میلیارد نفر هم برسد وجود دارد. افزایش تعداد کاربران این شبکه مجازی در حالی صورت می‌گیرد که انتقادهایی مبنی بر عدم رعایت و احترام حریم خصوصی از سوی مدیران این سایت مطرح شده است.
خبر قابل توجه در این هفته که کمتر رسانه داخلی به آن پرداخت راه‌اندازی موتور جست‌وجوی جدیدی به نام Taqwa.me یا همان تقوا برای رفع نیاز کاربران مسلمان و افرادی که به دنبال جست‌وجوی محتوای مربوط به دین اسلام هستند، بود که تا دو هفته دیگر روی شبکه جهانی وب مشاهده خواهد شد. آی‌تی‌پی گزارش داد این موتور جست‌وجو به طور آزمایشی از ماه مه در دسترس علاقه‌مندان قرار گرفته است و بازخوردهای ارائه‌شده از سوی کاربران در راستای اصلاح آن به‌کار گرفته شده است. مسوولان این موتور جست‌وجو بیان کرده‌اند به دنبال پشتیبانی و حمایت از جوامع مسلمان در سراسر جهان بوده و بخش عمده‌ای از درآمد خود را به ایجاد مدارس، ساخت تاسیسات درمانی و ساخت مساجد مختلف اختصاص خواهند داد.
پس از آنکه قائم‌مقام وزارت ارتباطات و فناوری اطلاعات خبر از راه‌اندازی اپراتور چهارم که البته در حوزه فناوری اطلاعات فعالیت خواهد کرد، داد، این هفته این مقام مسوول در تازه‌ترین اظهارنظر خود بیان کرد بنابر تصمیم وزارت ارتباطات قرار شد اپراتور چهارمی با نام اپراتور «فناوری اطلاعات» وارد بازار شود که حوزه فعالیت آن لایه دسترسی و فیبر نوری خواهد بود. مهدی اخوان‌بهابادی گفت با توجه به اینکه دولتی بودن اپراتور فناوری اطلاعات مغایر با کوچک‌سازی دولت و اصل ۴۴ است، بنابراین این اپراتور نمی‌تواند دولتی باشد و خصوصی خواهد بود. او مدعی شد سرعت دسترسی این اپراتور به اندازه‌ای خواهد بود که سرویس‌هایی نظیر IPTV بر روی این شبکه قابل ارائه باشد.
عضو شورای عالی انفورماتیک کشور ارزش خرید و فروش نرم‌افزار در جهان را حدود سه هزار میلیارد دلار در سال برآورد کرد اما از مقدار سهم ایران از این میزان حجم مبادلات سخنی نگفت. حسین طالبی تنها به این جمله بسنده کرد که ایران می‌تواند با توجه به مزیت‌هایی که دارد، سهم مناسبی از این بازار را در اختیار داشته

باشد. البته چندی قبل نایب‌رئیس اتحادیه صادرکنندگان نرم‌افزار از صادرات ۷۰ میلیون دلاری ایران در زمینه صادرات نرم‌افزار خبر داد. با این حال عضو شورای عالی انفورماتیک معتقد است سیاستگذاران و دولتمردان برنامه خاصی برای حمایت از صنعت نرم‌افزار و تولیدکنندگان داخلی ندارند و کشورمان با وجود پتانسیل‌های بسیار بالا در حوزه صنعت نرم‌افزار تاکنون نقشی در حوزه تولید و در تصاحب بازار بین‌المللی نداشته است.
به دلیل افت‌های مکرر شبکه اینترنت و کاهش سرعت، مسوولان شرکت ارتباطات زیرساخت تصمیم به افزایش تعداد خطوط STM1 گرفته و اعلام کردند پهنای باند اینترنت کشورمان از درگاه‌های بین‌المللی در شمال، غرب و جنوب کشور تامین می‌شود. سیدمحمد کاشانی مدیرکل بازرگانی و واگذاری مدارات شرکت ارتباطات زیرساخت گفت درگاه‌های بین‌الملل هم‌مرز با کشورهای عراق، ترکمنستان و افغانستان، مسیرهایی برای ترانزیت و فروش پهنای باند اینترنت به این سه کشور است.
سازمان تنظیم مقررات و ارتباطات رادیویی اعلام کرد، درصدد آن است تا مقررات تسهیل دسترسی و استفاده از شبکه سیم مسی در اختیار شرکت مخابرات را برای همه اپراتورها و شرکت‌هایی که به آن نیاز دارند، تنظیم کند. به گفته مسوولان این سازمان شبکه سیم مسی امکان واحدی در کشور است و فقط در اختیار شرکت مخابرات ایران قرار دارد و هیچ کس نه‌تنها نمی‌تواند شبکه‌ای به موازات آن ایجاد کند بلکه اصلاً اقتصادی و امکان‌پذیر هم نیست. از این رو سازمان تنظیم مقررات و ارتباطات رادیویی به این نتیجه رسیده است که مقرراتی را برای نحوه استفاده از این شبکه که در اختیار مخابرات ایران است، از نقطه صفری که یک شرکت می‌خواهد از این منبع استفاده کند، تنظیم کند. این قانون برای استفاده از شبکه مسی که PAPها و هر شرکت دیگری که در آینده به استفاده از این منبع نیاز داشته باشند، تدوین می‌شود و شرکت مخابرات ایران نیز ملزم است طبق این آیین‌نامه امکانات را در اختیارشان قرار دهد.
در این هفته مدیر ثبت دامنه‌های اینترنتی پژوهشگاه دانش‌های بنیادی از آخرین اقدامات برای کسب موافقت سازمان نظارت بر نام‌ها و ارقام اینترنتی نسبت به ثبت دامنه ملی «دات ایران» خبر داد. علیرضا صالح در ادامه همچنین بیان کرد تاکنون ۱۶۳هزار و ۵۹۱ دامنه اینترنتی در کشور به ثبت رسیده که ثبت دامنه با پسوند IR بیشترین آمار را دارد و ۱۵۳ هزار و ۷۳۲ سایت اینترنتی در کشور دارای پسوند لاتین IR هستند و دامنه ثبت‌شده با پسوند فارسی «ایران» حدود پنج هزار و ۱۴۹ دامنه است.

گیم‌نت

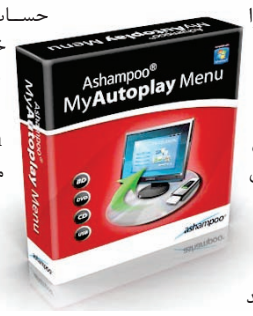
مبارزه با دیوان خبیث با «رویین‌تنی» از شاهنامه

زابل شهری است زیبا در سرزمین سیستان که قصر پیشداد حاکم سیستان و پدر آتار بر فراز آن بنا شده است. چندی است دیوان وحشی به ناحیه شمال غربی شهر حمله کرده و آنجا را به خاک و خون کشیده‌اند. پیشداد و آتار با کیاست و شجاعت بی‌نظیر خود باید شهر را از این وضعیت نجات دهند. بازی «رویین‌تنی» که داستان آن در فضای اساطیری شاهنامه فردوسی روی می‌دهد، قسمت دوم از بازی «عصر پهلوانان» است (در سال گذشته به بازار عرضه شد) که اینک روانه بازار شده است. این بازی برای گروه سنی ۱۵+ (بالای ۱۵ سال) طراحی شده است. در این بازی نیز مبارزه «آتار و ویراجا» ادامه می‌یابد که اولی شاهزاده جوان و پسر پیشداد حاکم وقت زابل، و «ویراجا» موجودی عجیب و خبیث است. محور داستان این بازی حول کشمکش و نبرد نیروهای خیر و شر برای رسیدن به راز رویین‌تنی دور می‌زند و هر یک از شخصیت‌ها تلاش می‌کند با دستیابی به راز جاودانگی برای همیشه از هر نوع گزند و آسیبی در امان بمانند. «آتار» طی این مسیر با سرزمین‌های جدید و شخصیت‌های عجیبی روبه‌رو می‌شود. سرزمین سیستان (زابل)، منطقه کولی‌ها، سرزمین بیابانی، شهر پریان، غار خمشدای، سرزمین آتشفشانی، سرزمین مردوش و غار کوتوله‌ها نام سرزمین‌های جدیدی هستند که باید آتار از آنها بگذرد. ایلاریل ملکه پریان، نوتریل پری، سیلماریل دختر ملکه پریان و... از جمله شخصیت‌هایی هستند که در این بازی با آنها روبه‌رو خواهیم شد. در این بازی بازیکن برای حل مسائل و خطراتی که با آنها مواجه می‌شود ضمن به‌کارگیری نیروهای ماورایی و سلاح‌های متنوع باید از هوش و درایت خود نیز بهره گیرد. در این بازی شما یک کوله‌پشتی را حمل می‌کنید که در آن بیش از ۱۲۰ آیتم می‌توانید در کل روند بازی به آن اضافه شود. آیتم‌ها در چهار دسته سلاح‌ها، دفاعی، سلامتی و خاص قرار می‌گیرند که بسته به نوع، قابل غلاف کردن، انداختن، عدم استفاده یا خرید و فروش هستند. همچنین هر نیروی ماورایی آیتم مخصوص به خود را دارد که آنها را باید از افرادی خاص در خلال انجام ماموریت‌ها به دست آورد. مانا عامل کنترل‌کننده این نیروهاست. هرچه که بیشتر از این نیروها در راستای ضربه زدن به دشمن‌ها استفاده کنید، فره ایزدی بالاتر رفته، زمان احیای مانا کوتاه‌تر می‌شود. در نهایت اینکه در قسمت دوم بازی عصر پهلوانان، داستان مبارزه آتار و ویراجا برای دست یافتن به گنجینه‌های رویین‌تنی ادامه می‌یابد. در این قسمت، دیوان پیش روی بیشتری در شهر زابل وجود دارند و خطر سقوط، هر لحظه این شهر را تهدید می‌کند. در این بازی همانند بیشتر بازی‌ها نقش محوری بازیکن در طول بازی رشد کرده و توانایی‌های او افزایش می‌یابد.

دنیای نرم‌افزار

ساخت اتوران‌های زیبا به کمک نرم‌افزار

شرق: مطمئناً شما نیز با سی‌دی‌هایی که با قرار دادن در سی‌دی درایو به صورت خودکار اقدام به باز کردن پنجره‌ای برای کاربر می‌کنند روبه‌رو شده‌اید. به این عمل و برنامه‌هایی که به این شکل است اتوران (Autorun) می‌گویند.
طراحی و ساخت اتوران‌ها به منظور راحتی بیشتر کاربران با سی‌دی‌هاست. به عنوان مثال در بسته نرم‌افزاری که شامل چندین سی‌دی است و در هر یک از آنها تعداد زیادی از نرم‌افزارها قرار گرفته توسط اتوران‌ها، این برنامه‌ها لیست می‌شوند و اسامی هر یک از آنها به خود نرم‌افزار لینک شده تا کاربر به راحتی برنامه مورد نظر خود را یافته و آن را در کوتاه‌ترین زمان ممکن نصب کند. همچنین از اتوران‌ها می‌توان در ساخت سی‌دی‌های آموزشی نیز بهره برد. قرار دادن تصاویر و فیلم‌های آموزشی به همراه آموزش‌ها به شکل چندرسانه‌ای در جذب مخاطب و همچنین یادگیری آسان‌تر مطالب برای کاربر تاثیرگذار است.
برای ساخت اتوران‌ها از نرم‌افزارهای مختلفی می‌توان استفاده کرد که توسط تولیدکنندگان دنیای نرم‌افزاری برای کاربران ساخته شده است. به همین علت در این مطلب سعی داریم شما را با قوی‌ترین نرم‌افزار در این خصوص آشنا کنیم.



My Autoplay Menu نام نرم‌افزاری است که به کمک آن کاربران قادر خواهند بود اتوران‌های مورد نظر را با سلیقه خود طراحی کنند. از دیگر استفاده‌های A - torun می‌توان به مثالی دیگر اشاره داشت. فرض کنید قصد دارید در سیستم یکی از دوستان خود فایلی را به صورت مخفیانه اجرا کنید. به عنوان مثال قصد دارید فایل سرور یک تروجان را بر روی سیستم دوست خود اجراکنید.تبلهکامپیوتراننفوذکنید
با ساخت یک autorun ساده و قرار دادن فایل مربوطه در آن و قرار دادن آن در سی‌دی به راحتی فایل موردنظر را به صورت مخفیانه در سیستم قربانی خود اجرا کنید. برای این کار تنها نیاز است سی‌دی را در سی‌دی درایو قرار داده و منتظر بمانید که autorun شما به همراه فایل مربوطه اجرا شود و با این کار مشاهده خواهید کرد که عملیات مورد نظر به راحتی انجام شده است.
این نرم‌افزار دارای ویژگی‌های بسیاری است که از جمله می‌توان به این موارد اشاره داشت:
- قابلیت ساخت autorun برای دی‌وی‌دی و سی‌دی و همچنین حافظه‌های جانبی فلش (USB Flash Drive)
- اجرای نرم‌افزارها به صورت خودکار و ده‌ها امکانات دیگر.
به هرحال اگر شما جزء آن دسته از کاربرانی به حساب می‌آیید که علاقه‌مند هستید برای خود اتوران‌های مورد نظر با سلیقه خود طراحی کنید به شما توصیه می‌کنیم حتماً سری به سایت p30world.com بزنید تا به راحتی نرم‌افزار مورد نیاز این کار را به طور رایگان در سیستم خود بارگذاری کنید. گفتنی است این نرم‌افزار محصولی از شرکت Ashampoo Software به شمار می‌آید.