خبر

آیین‌نامه نظارت بر شبکه‌های خدمات پستی تدوین می‌شود

■ آیین‌نامه نظارت بر شبکه‌های خدمات پستی در بخش دولتی و خصوصی از سوی معاونت نظارت و اعمال مقررات رگولاتوری تدوین می‌شود. به گزارش روابط عمومی سازمان تنظیم مقررات و ارتباطات رادیویی حسن رضوانی معاون نظارت و اعمال مقررات این سازمان ضمن بیان این مطلب گفت: این آیین‌نامه به منظور ساماندهی شبکه پست در بخش‌های خصوصی و دولتی تدوین می‌شود و مناطق هفتگانه رگولاتوری باید بر این شبکه‌ها نظارت داشته باشند. او افزود: تقویت بخش رگولاتوری پست از سیاست‌های کلی سازمان تنظیم مقررات و ارتباطات رادیویی در سال جاری است.

ظرفیت اینترنت بین‌الملل ایران افزایش یافت

■ ظرفیت اینترنت بین‌الملل شرکت ارتباطات زیرساخت ۳۲ لینک STM۱ افزایش یافت. به گزارش دفتر روابط عمومی و امور بین‌الملل شرکت ارتباطات زیرساخت، «احمد پورنگ نیا» عضو هیات مدیره این شرکت با اعلام این مطلب افزود: با توسعه دولینک STM16 ظرفیت اینترنت کشورمان به ۲۰۵ لینک STM1 رسید. پورنگ نیا با اشاره به این نکته که این میزان افزایش ۱۸ درصد رشد را نشان می‌دهد، اضافه کرد: این ظرفیت به مشتریانی که با زیرساخت قرارداد دارند، واگذار خواهد شد. عضو هیات مدیره شرکت ارتباطات زیرساخت اضافه کرد: این میزان افزایش بخشی از برنامه توسعه شرکت ارتباطات زیرساخت در ارتقا پهنای باند اینترنت کشور در سال جاری است و توسعه‌های جدیدی در این زمینه در راه است که به زودی اعلام خواهد شد.

برترین شرکت‌های اینترنتی اعلام شدند

■ فهرست شرکت‌های برتر ارایه‌دهنده خدمات اینترنتی کشور در فروردین‌ماه منتشر شد. به گزارش مرکز مدیریت توسعه ملی اینترنت (متما) که زیرنظر سازمان فناوری اطلاعات فعالیت دارد، ماهانه به انتشار گزارش‌هایی درباره برترین شرکت‌های ارایه‌دهنده خدمات اینترنتی می‌پردازد. علاوه بر این، با مراجعه به سایت متما می‌توان برای سنجش و تست سرعت اینترنت خود با اتصال به نزدیک‌ترین سرور، به میزان سرعت واقعی اتصال خود به اینترنت پی برد و در این نوع آزمایش کاربران با استفاده از مرورگر خود به سرور سنجش متصل شده و دو طرف نرم‌افزار سنجش (Client Side و Server Side) با تبادل بسته‌های مشخصی از اطلاعات و زمان‌بندی ارسال و دریافت بسته‌ها متوسط سرعت اتصال کاربر را محاسبه می‌کند. تست‌های این مرکز روی دو بازه تست‌های کمتر از ۵۱۲ کیلوبایت بر ثانیه و تست‌های ۵۱۲ تا دو مگابایت بر ثانیه انجام می‌شود که نتایج ده‌تایی‌های برتر به دست آمده، مشخص شده است. در نتایج تست‌های کمتر از ۵۱۲ کیلوبایت بر ثانیه در بازه زمانی ساعت یک بامداد تا هشت صبح، به ترتیب شرکت‌های شاتل، ارتباطات مبین‌نت و پارس آنلاین و در بازه زمانی ساعت هشت صبح تا ۱۶ شرکت‌های شاتل، پیشگامان توسعه ارتباطات، آریا سپهر، پارس آنلاین، نداگستر صبا، ارتباطات مبین نت، رسپینا، عصر انتقال داده‌ها و افرانت و در بازه زمانی ۱۶ تا ۲۵ شرکت‌های شاتل، نداگستر صبا، پارس آنلاین، ارتباطات مبین نت و افرانت در رده برترین‌ها قرار گرفتند. در نتایج تست‌های ۵۱۲ کیلوبایت بر ثانیه تا ۲ مگابایت بر ثانیه نیز در بازه زمانی ساعت یک بامداد تا هشت صبح، شرکت‌های توسعه رسان پاسارگاد، شبکه ارتباط شبدیز، شاتل، پارس آنلاین و نداگستر صبا، در بازه زمانی هشت صبح تا ۱۶ شرکت‌های شبکه ارتباط شبدیز، توسعه رسان پاسارگاد، شاتل، پارس آنلاین، عصر انتقال داده‌ها و نداگستر صبا و در بازه زمانی ۱۶ تا ۲۴ شرکت‌های پارس آنلاین، نداگستر صبا و شاتل بهترین کیفیت و سرعت خدمات ارایه شده را دارا بوده‌اند.

راه‌اندازی ۱۱ مرکز داده در ۱۱ استان

■ مناقصه ایجاد و راه‌اندازی ۱۱ مرکز داده در ۱۱ استان کشور برگزار شده و نتایج نهایی آن تا پایان ماه جاری مشخص خواهد شد. به گزارش روابط عمومی سازمان فناوری اطلاعات، مدیر کل دفتر تحقیق و توسعه سازمان فناوری اطلاعات ضمن بیان این مطلب افزود: این مراکز به صورت پردازش ابری راه‌اندازی و به منظور اتصال به شبکه ملی اطلاعات استفاده خواهند شد. هادی ملکی پرست، گفت: استان‌های مشهد، مرکزی، شیراز، گرگان، همدان، اهواز، قم و کرمان از جمله استان‌هایی هستند که عملیات زیرساختی و تامین تجهیزات مورد نیاز برای راه‌اندازی مراکز داده در آنها اجرا می‌شود. او اضافه کرد: مراکز داده در برخی استان‌ها پیش از این راه‌اندازی شده یا زیرساخت‌های لازم برای راه‌اندازی این مراکز ایجاد شده بود که باید به منظور ایجاد قابلیت اتصال به بقیه سرورها این مراکز تکمیل و به روزرسانی شود که استان‌های اصفهان، بوشهر و تبریز از آن جمله محسوب می‌شوند. هادی ملکی پرست با بیان این مطلب که ایجاد این مراکز داده با حمایت وزارت ارتباطات و فناوری اطلاعات و از طریق بخش خصوصی اجرا می‌شود، تصریح کرد: بر اساس برنامه زمانبندی شده، تا پایان سال جاری ایجاد این مراکز نهایی خواهد شد و به بهره‌برداری می‌رسد.

حملات سایبری، راهکار مشترک آمریکا و رژیم صهیونیستی

بدافزارها توپخانه‌های جدید دشمن

محمود حبیبی

چندی قبل «غلامرضا جلالی» رییس سازمان پدافند غیر عامل ایران از شناسایی بدافزاری به نام «استارس» خبر داد که محققان ایرانی پس از بدافزار استاکسنت موفق به شناسایی آن شدند. انتشار این خبر به فاصله چند ماه بعد از انتشار خبر حمله سایبری به نیروگاه نطنز بازتاب فراوانی در رسانه‌های جهانی داشت و بار دیگر ضرورت مقابله با تهدیدات حملات سایبری در جهان امروز را مشخص کرد. بررسی‌های مختلف نشان می‌دهند که این نوع بدافزارها کار هکرهای عادی نیست و طراحی آنها مستلزم داشتن اطلاعات بعضا محرمانه فراوانی است که فقط برخی دولت‌ها قادر به دسترسی به آنها هستند. نوشته زیر که در واقع ترجمه مطلبی است که برای اولین‌بار در روزنامه نیویورک تایمز منتشر شد، ابعاد این حمله و حملات مشابه را مورد بررسی قرار داده است.

آزمایش‌های محرمانه در دیمونا

«مجتمع دیمونا» در صحرای «نقب» به مرکز حساس برنامه تسلیحات اتمی رژیم صهیونیستی معروف است؛ مساله‌ای که آنها هرگز به آن اقرار نکرده‌اند اما این مجتمع شامل مجموعه‌ای گسترده از کارخانه‌هایی است که سوخت مصرفی زرادخانه اتمی رژیم صهیونیستی را تامین می‌کنند. اما به گفته کارشناسان نظامی و اطلاعاتی آگاه به امور عملیات دیمونا، این مرکز در طول دو سال گذشته یک کارکرد جدید و البته محرمانه یافته است: مرکز آزمایش‌های حساس آمریکا و رژیم صهیونیستی برای پروژه‌های مقابله با برنامه اتمی ایران.

کارشناسان اتمی معتقدند پشت سیم‌های خاردار دیمونا، رژیم صهیونیستی اقدام به نصب و راه‌اندازی سانتریفیوژهای اتمی مشابه سانتریفیوژهای فعال ایرانی در نیروگاه نطنز کرده است. آنها می‌گویند: دیمونا مدت‌هاست سرگرم آزمایش روی بدافزار استاکسنت است. استاکسنت یک نرم‌افزار ویرانگر رایانه‌ای است که برای از کار انداختن برنامه هسته‌ای ایران طراحی شده‌است، البته مقام‌های ایرانی اعلام کرده‌اند در زمان مناسب متوجه این بدافزار شده و توانسته‌اند آن را خنثی کنند. یک کارشناس آمریکایی در امور اطلاعات اتمی می‌گوید: «برای آزمایش این کرم رایانه‌ای، باید ابتدا شناخت دقیق از سیستم‌های فعال اتمی داشت و یکی از دلایلی که این بدافزار تا حدی موفق به اخلال در سانتریفیوژهای اتمی شد، این بود که رژیم صهیونیستی قبلا آن را دقیقا روی سانتریفیوژهای مشابه آزمایش کرده بود.» هرچند مقام‌های آمریکا و رژیم صهیونیستی از اظهارنظر عمومی درباره آزمایش‌های دیمونا خودداری می‌کنند اما تحرکات در دیمونا و همین طور تلاش‌های مشابه در آمریکا در واقع آخرین و محکم‌ترین شواهدی هستند که نشان می‌دهند این ویروس به عنوان یک پروژه آمریکایی/اسراییلی برای اختلال در برنامه‌های اتمی طراحی شده‌است.

ارزیابی‌های جدید

در سال‌های اخیر، «میر داگان» رییس سازمان اطلاعاتی موساد که در شرف بازنشستگی است و هیلاری کلینتون وزیر خارجه آمریکا در اظهارنظرهای جداگانه مدعی شده‌اند که به اعتقاد آنها برنامه اتمی ایران با مشکلاتی مواجه شده است. کلینتون دلیل این امر را تحریم‌های آمریکا اعلام کرد که به ادعای او توانایی ایران را برای خرید تجهیزات فنی و تعاملات تجاری با جهان محدود کرده است. کارشناسی از اروپا و آمریکا که تاکنون بدافزار استاکسنت را بررسی کرده‌اند، در مصاحبه‌های متعدد در طول سه ماه گذشته اعلام کردند که این بدافزار بسیار پیچیده و دقیق‌تر از چیزی است که در ابتدا تصور می‌شد. البته هنوز ابهام‌های فراوانی در مورد این بدافزار وجود دارند که مهم‌ترین آنها این است که دقیقا چه کسی این کرم رایانه‌ای را طراحی کرده است. به نظر می‌رسد چندین نفر از کشورهای مختلف در ساخت این بدافزار نقش داشته‌اند.

زیمنس و شکاف‌های امنیتی

در اوایل سال ۲۰۰۸، شرکت صنعتی زیمنس آلمان برای شناسایی ضعف کنترل کنندگان رایانه‌ای خود باب همکاری را با یکی از لابراتورهای ملی آمریکا در «آیداهو» آغاز کرد. زیمنس یکی از سازندگان و فروشندگان بزرگ تجهیزات صنعتی در سراسر جهان است. سازمان اطلاعاتی آمریکا می‌دانست که تجهیزات زیمنس در نطنز مورد استفاده قرار گرفته‌اند. زیمنس می‌گوید، این همکاری بخشی از برنامه‌های عادی این شرکت برای محافظت از تولیدات خود در برابر حملات سایبری بوده است. با وجود این، زیمنس عملا این امکان را به لابراتور آیداهو ـ که زیر نظر وزارت انرژی آمریکا و مسوول کنترل تسلیحات اتمی آمریکا است ـ داد که شکاف‌های پنهان سیستم‌های زیمنس را شناسایی کنند؛ شکاف‌هایی که استاکسنت سال بعد از طریق همان‌ها وارد عمل شد.

استاکسنت از دو بخش اساسی تشکیل شده است. یک بخش مخصوص اختلال در سانترفیوژهای اتمی ایران طراحی شده‌اند و بخش دیگر بسیار مرموز است. بدین صورت که یک برنامه رایانه‌ای است که می‌تواند به صورت محرمانه عملیات عادی یک نیروگاه اتمی را ثبت کند و سپس هنگامی که با صدور چندین دستور این عملیات مختل شد اقدام به ارایه اطلاعات غلط به اپراتور کند طوری که او متوجه این اختلال نشود. اما حمله استاکسنت به ایران موفق نبوده است. برخی کارشناسان معتقدند این کرم عملا بذرهایی را برای حملات دیگر کاشته است. رالف لانگنر، کارشناس امنیت رایانه‌ای در هامبورگ آلمان - که از اولین کارشناسانی بود که شروع به رمزگشایی از استاکسنت کرد- می‌گوید: «این نوع حملات عملا شکل جدیدی از جنگ افزار صنعتی را وارد عمل کرده است که خود آمریکا در برابر آن بسیار آسیب‌پذیر است.»

پروژه مشترک آمریکا و اسراییل

البته نه مقام‌های آمریکایی و نه رژیم صهیونیستی هیچ کدام هنوز رسما حتی نام استاکسنت را نیز به زبان نیاورده‌اند چه برسد به اینکه به نقش خود در طراحی آن اشاره کنند. وقتی از مقام‌های اسراییلی درباره تاثیرات این حمله سوال می‌شود، صرفا لبخند می‌زنند. «گری سامور» استراتژیست اصلی باراک اوباما، رییس جمهور آمریکا در زمینه مقابله با تسلیحات کشتار جمعی اخیرا در نشست خبری درباره ایران از پاسخ به سوالی درباره استاکسنت طفره رفت اما با لبخندی بر لب گفت: «خوشحالم که می‌شنوم آنها با سانتریفیوژهای خود مشکل پیدا کرده‌اند و آمریکا و هم‌پیمانانش هر کاری از دست‌شان برمی‌آید انجام می‌دهند تا این مشکل پیچیده‌تر شود.» در روزهای اخیر، مقام‌های آمریکایی که خواستند نام‌شان فاش نشود، در مصاحبه‌های مختلف گفتند که به اعتقاد آنها درباره تاثیرات این بدافزار آن‌طور که باید سخن گفته نشده‌است.

> **آمریکا بعد از آنکه لیبی برنامه اتمی خود را در اواخر سال ۲۰۰۳ متوقف کرد و تجهیزات اتمی خود را تحویل داد؛ آمریکا آنها را به لابراتوار ملی خود در تنسی منتقل کرد و در اینجا بود که دانشمندان اتمی آمریکا با نسل اول سانتریفیوژها آشنا شدند**

اما گزارش برخی از دانشمندان رایانه‌ای، کارشناسان غنی‌سازی اتمی و مقام‌های سابق حاکی از آن است که رقابتی پنهانی بین آمریکا و رژیم صهیونیستی برای ساخت و طراحی استاکسنت وجود داشته و این در واقع یک پروژه مشترک بین آمریکا و رژیم صهیونیستی بود که البته برخی از کارشناسان آلمانی و انگلیسی نیز خواسته یا ناخواسته در این پروژه همکاری داشتند. ریشه‌های سیاسی این پروژه را می‌توان در آخرین ماه‌های حضور جرج بوش از قدرت جست‌وجو کرد. در ژانویه ۲۰۰۹، روزنامه نیویورک تایمز گزارش داد که آقای بوش دستور اجرای یک برنامه محرمانه را برای اختلال در سیستم‌های رایانه‌ای و الکتریکی صادر کرده است. باراک اوباما حتی قبل از اینکه رسما وارد کاخ سفید شود در جریان این برنامه قرار گرفت و به گفته منابع آگاه حتی خواستار تسریع در اجرای آن نیز شد. منابع دیگر نیز حاکی است رژیم صهیونیست نیز بسیار در این برنامه جدی بوده است. آنها مدت‌ها در پی یافتن راهی برای مقابله با توان اتمی ایران با پرداخت کمترین هزینه یا جنگ بودند و برخلاف برخی گزارش‌ها نمی‌خواستند حملاتش را به تاسیسات اتمی عراق در سال ۱۹۸۱ و سوریه در سال ۲۰۰۷ تکرار کنند. اما آمریکا با این نوع حملات اساسا مخالف بود تا اینکه اسراییل اعلام کرد راه مورد نظر خود را یافته است و این برنامه را پیشنهاد کرد. در واقع اظهارات داگان که چنین چیزی را نشان می‌دهد. ظاهرا دولت اوباما نیز به نتیجه مشابهی رسیده بوده‌است.

سال‌های پیش از حمله استاکسنت به ایران، واشنگتن عمیقا نگران آسیب پذیری میلیون‌ها رایانه‌ای بود که همه چیز را در آمریکا تنظیم می‌کنند، از تعاملات بانکی گرفته تا شبکه‌های برق. رایانه‌های موسوم به «کنترل کننده‌ها» همه تجهیزات صنعتی را اداره می‌کنند. تا اوایل ۲۰۰۸ سازمان امنیت داخلی آمریکا همکاری خود را با لابراتوار ملی آیداهو برای تحقیقات درباره کنترل کننده‌های مختلف زیمنس موسوم به P.C.S-۷ شروع کرده بود. نرم‌افزار پیچیده این کنترل کننده‌ها موسوم به Step ۷ می‌تواند مجموعه‌ای از ابزارهای صنعتی، حسگرها و ماشین‌آلات را همزمان مدیریت کند. آسیب‌پذیری کنترل کننده‌ها در برابر حملات سایبری یک راز آشکار بود. در جولای ۲۰۰۸ لابراتوار آیداهو و زیمنس درباره نقاط آسیب پذیری کنترل کننده به نتایج مهمی رسیده بودند که در قالب گزارشی در یک کنفرانس علمی در شیکاگو در معرض دید کارشناسان قرار گرفت.

> **گزارش برخی از دانشمندان رایانه‌ای، کارشناسان غنی‌سازی اتمی و مقام‌های سابق حاکی از آن است که رقابتی پنهانی بین آمریکا و رژیم صهیونیستی برای ساخت و طراحی استاکسنت وجود داشته و این در واقع یک پروژه مشترک بین آمریکا و رژیم صهیونیستی بود**

در این گزارش ۶۲ صفحه‌ای ضمن تشریح انواع راه‌های نفوذ در شکاف‌های سیستمی زیمنس اعلام شده بود که حمله کنندگان هدفشان کنترل سیستم‌های کنترلی است. البته لابراتوار آیداهو در این گزارش برخی سوالات را بی‌پاسخ گذاشت. در ابتدا هدف از این همکاری را شناسایی نقاط ضعف سیستم‌های زیمنس اعلام کرد اما افزود؛ بنا به دلایل امنیتی نمی‌تواند درباره اهداف محرمانه خود اظهارنظر کند، یعنی اینکه معلوم نیست آیا یافته‌های خود را درباره این سیستم‌ها در اختیار سازمان‌های اطلاعاتی آمریکا قرار داده است یا خیر. این گزارش که در وب‌سایت زیمنس منتشر شده بود اخیرا حذف شد. یکی از موارد تحریم‌ها علیه ایران مخالفت با صادرات سیستم‌های کنترلی و رگولاتورهای الکتریکی زیمنس بود. بر اساس اسناد محرمانه وزارت خارجه آمریکا که در وب سایت ویکی لیکس منتشر شد، دولت امارات عربی متحده در آوریل سال ۲۰۰۹ مانع از ارسال ۱۱۱ جعبه حاوی این سیستم‌ها از بندر دوبی به بندر عباس در جنوب ایران شد.

رمزگشایی از استاکسنت

هیچ کس بیشتر از آقای لانگنر پیگیر این مساله نبود. او یک روان‌شناس قدیمی است که اکنون مدیریت یک شرکت امنیت رایانه‌ای را در حومه هامبورگ در اختیار دارد. او که مشتاق طراحی یک نرم‌افزار حمایتی برای مشتریان خود بود به اتفاق پنج کارمند خود شروع به رمزگشایی این بدافزار و اجرای آن روی سیستم‌های کنترلی زیمنس کرد. در حین آزمایش‌های مختلف او ناگهان متوجه شد که این کرم فقط وقتی فعال می‌شود که در پیکربندی خاصی از کنترل کنندگان که عمدتا در نیروگاه‌های سانتریفیوژی وجود دارند، قرار گیرد. او گفت: البته اجرای این کار مستلزم دقت فراوانی است. برای مثال، یک بخش کوچک از این بدافزار عمدتا برای ارسال دستور به ۹۸۴ دستگاه استفاده می‌شود که با یکدیگر مرتبط هستند. جالب اینکه وقتی بازرسان بین‌المللی در اواخر سال ۲۰۰۹ از ایران بازدید کردند متوجه شدند که ایران مجموعا ۹۸۴ دستگاه خود را که در تابستان قبل فعال بودند، از رده خارج کرده‌است.

اما همانطور که لانگنر به تحقیقات خود ادامه می‌داد؛ متوجه یک روند جالب شد که او نامش را «کلاهک دوگانه» گذاشت و منظور از آن بخشی از این بدافزار است که می‌تواند تا مدت‌ها غیرفعال باقی بماند اما کمی بعد با صدور فرمان به دستگاه‌ها طوری آنها را به حرکت درآورد که عملا پروانه سانتریفیوژها از کار بیفتد. یک بخش دیگر موسوم به «عامل میانی» نیز وجود دارد که اقدام به ارسال سیگنال‌های غلط به سیستم محافظتی می‌کند تا متوجه اخلال در سیستم نشود و فرض را بر این بگذارد که همه چیز عادی است. لانگنر بعدها نوشت: «تحلیل رمزهای این بدافزار نشان می‌دهد که استاکسنت صرفا ارسال یک پیام یا اثبات یک مفهوم نیست.» او بلافاصله افزود: «نگارش این بدافزار کار هکرها نیست. بلکه کار کسی است که کنترل کنندگان زیمنس را خوب می‌شناسد و یک شناخت دقیق از کارکرد غنی‌سازی دارند.» یعنی همان مواردی که آمریکا و رژیم صهیونیستی دقیقا به آنها آگاهی داشتند.

محرمانه استاکسنت

شاید محرمانه‌ترین بخش ماجرای استاکسنت این باشد که چگونه ممکن است این بدافزار قبلا آزمایش شده باشد. ماجرا از هلند آغاز می‌شود. در اواخر دهه ۱۹۷۰ این کشور یک دستگاه مرتفع را برای غنی‌سازی اختراع کرد. گفته می‌شود «عبدالقدیرخان» دانشمند اتمی پاکستان که در آن زمان برای این شرکت کار می‌کرد، این طرح را سرقت کرد و در سال ۱۹۷۶ به پاکستان گریخت. این دستگاه موسوم به P-۱ که در واقع نسل اول سانتریفیوژهای پاکستان است به این کشور این امکان را داد که به بمب اتمی دست یابد و وقتی عبدالقدیرخان بعدها بازار سیاه اتمی خود را راه انداخت به صورت غیرقانونی P-۱ را به کره شمالی و لیبی منتقل کرد.

P-۱ بیش از شش فوت ارتفاع دارد. در داخل آن یک پروانه آلومینیومی قرار دارد که گاز اورانیوم را با سرعتی خیره‌کننده تولید و اورانیوم لازم را برای تامین سوخت رآکتورهای اتمی یا ساخت بمب اتمی تامین می‌کند.

آونر کوهن نویسنده کتاب «محرمانه‌ترین راز» (۲۰۱۰) می‌گوید: «من اطلاعات خاصی درباره استاکسنت ندارم اما دست اسراییل را در این ماجرا می‌بینم و معتقدم که دانش سانتریفیوژی برای طراحی این بدافزار حیاتی است.»

یک پای دیگر ماجرا، آمریکاست. این کشور بعد از آنکه لیبی برنامه اتمی خود را در اواخر سال ۲۰۰۳ متوقف کرد و تجهیزات اتمی خود را تحویل داد؛ آنها را به لابراتوار ملی خود در تنسی منتقل کرد و در اینجا بود که دانشمندان اتمی آمریکا با نسل اول سانتریفیوژها آشنا شدند. تا اوایل سال ۲۰۰۴ طیف متنوعی از کارشناسان اتمی خصوصی و فدرال در آمریکا که زیر نظر سازمان اطلاعات مرکزی دور هم جمع شده بودند، از دولت این کشور خواستند که یک نیروگاه اتمی محرمانه بسازد که در آن بتوانند P-۱ را راه‌اندازی و نقاط ضعف و قوت آن را بررسی کنند، بنابراین نقش این نیروگاه محرمانه را در طراحی استاکسنت نباید از نظر دور داشت. اما در این میان یک مشکل وجود داشت و آن اینکه آمریکا و همپیمانانش با مشکلاتی فنی مواجه بودند از این نظر که P-۱ که یک دستگاه مرتفع و بسیار پیچیده است دارای طراحی خاصی است که به راحتی نمی‌توان به اصول آن پی برد. جالب اینکه مسوولان لابراتوار تنسی حتی به همکاران انگلیسی خود نیز متوسل شدند و با ارسال برخی از تجهیزات این دستگاه از آنها مشاوره خواستند اما از قرار معلوم دانشمندان انگلیسی نیز نتوانستند تمام و کمال سیستم و مکانیسم این دستگاه را شناسایی کنند.

ایرانی‌ها در خاورمیانه نخستین میزبان شدند

نسل جدید تلویزیون هوشمند و سینما سه‌بعدی

شرکت کره‌ای ال‌جی، تلویزیون هوشمند و سینما سه‌بعدی خود را برای اولین بار در منطقه خاورمیانه و آفریقای شمالی به بازار ایران فرستاد. مدیران ال‌جی و گلدیران در نشست خبری مشترک، تلویزیون‌های 3D Smart TV، CINEMA و نسل جدید عینک‌های سه‌بعدی سبک و ارزان‌قیمت ال‌جی را معرفی کردند.

سینما سه‌بعدی

Lw5700 و lw6510 اولین تلویزیونی‌های سه‌بعدی در دنیا هستند که تصویر سه‌بعدی بدون پرش آنها از طرف موسسات معتبری چون TUV و Intertek تایید شده است و می‌توانید مدت زمانی طولانی بدون سرگیجه و خستگی چشم، تصاویر سه‌بعدی را مشاهده کنید.

عینک‌های تلویزیون سینما سه‌بعدی قیمت مناسب دارد که معادل ۲۰ درصد قیمت عینک‌های متداول در بازار است. شرکت ال‌جی امکانی را در تلویزیون‌های سینما سه‌بعدی خود قرار داده که قادر است تصاویر دو بعدی را به تصاویر سه‌بعدی تبدیل کند. تکنولوژی پنل‌های مخصوص ال‌جی در این تلویزیون باعث می‌شود که فرمت تصاویر سه‌بعدی منحصرا صورت گیرد و نیازی به مطابقت با عینک‌های سه‌بعدی نداشته باشد. برخورداری از زاویه دید ۱۸۰ درجه در این دستگاه به افراد امکان می‌دهد که در هر کجا دوست دارند نشسته و بدون هیچ نگرانی به تماشای تلویزیون بپردازند.

تلویزیون هوشمند

کاربران در تلویزیون هوشمند، تنها در یک صفحه می‌توانند به راحتی به تمام ویژگی‌ها و سرگرمی‌های متنوع دسترسی داشته و هر آنچه را که دوست دارند، مشاهده کنند. این صفحه اصلی به کاربران امکان می‌دهد که به سادگی محتوای مورد علاقه خود مانند پخش زنده تلویزیون، بازی‌ها و برنامه‌ها، سرویس‌های منتخب و نوار دسترسی را انتخاب و مشاهده کنند. همچنین با استفاده از ویژگی «حرکت دست و کلیک هنگام مشاهده» می‌توانید بدون نگاه کردن به کنترل آنچه را که دوست دارید جابه‌جا کرده و انتخاب کنید. این کنترل جادویی شبیه ماوس عمل می‌کند و دارای یک نشانگر روی صفحه است.

کاربران هنگام استفاده از آن احساس راحتی بیشتری نسبت به کنترل‌های معمولی دارند. علاوه بر این اشتراک‌گذاری هوشمند ال‌جی به شما امکان می‌دهد که از طریق USB، DLNA و Media Link به راحتی محتوا و فایل مورد نیاز خود را از هر دستگاه دیجیتالی به تلویزیون انتقال دهید.

همچنین با استفاده از Media Link کاربران Smart TV ال‌جی می‌توانند به راحتی محتوا و فایل‌های کامپیوتر خود را به تلویزیون منتقل کنند و به آنها دسترسی داشته باشند. داریوش مهرجویی، مسعود جعفری‌جوزانی و علی معلم میهمانان هنری ویژه این نشست بودند که درباره فناوری جدید سه‌بعدی تلویزیون ال‌جی سخنرانی کردند.

داریوش مهرجویی در این مراسم اعلام کرد که با ورود این فناوری برای ساخت یک فیلم سه‌بعدی برنامه‌ریزی می‌کند. در ادامه حسین تنهایی، قائم‌مقام مدیر عامل گلدیران نیز وعده داد که داریوش مهرجویی نخستین فیلم سه‌بعدی در ایران را با همکاری ال‌جی خواهد ساخت.

نگاه

دنیای دیجیتال و مرگ اسامه

■ فراگیرشدن اخبار کشته‌شدن بن‌لادن در حالی موجب بمباران متن‌ها و تصاویری در اینترنت و توییتر شد که نمونه‌ای از این رویداد دیجیتالی قبلا نیز با مرگ مایکل جکسون یا بیلی میز به وقوع پیوسته بود. انتشار اعلامیه‌های مرگ افراد یکی از طلسم‌های بزرگ وب سایت توییتر است. انتشار اخبار مربوط به مرگ جف گلد بلام، بازیگر باعث شد توییت‌های فراوانی در این زمینه در این وب سایت میکرو بلاگینگ سرازیر شوند که به سختی می‌توان در مورد جزییات و تعداد آنها سخن گفت. خبر عملیاتی که منجر به مرگ اسامه بن‌لادن در پاکستان شد، اولین بار در سایت توییتر منتشر شد. یک مشاور آی‌تی که در ابیت‌آباد پاکستان زندگی می‌کند، بدون آنکه متوجه باشد، جزییات عملیات تحت رهبری آمریکا علیه اسامه بن‌لادن را در سایت توییتر منتشر کرد که پس از آن به تایید ریاست جمهوری ایالت متحده رسید. بنا بر گزارش‌های سایت‌های مختلف، ترافیک اینترنتی سایت‌های فیس بوک و توییتر نیز نسبت به روز جمعه عروسی سلطنتی بریتانیا، به میزان قابل توجهی بیشتر بود. در ساعت ۱۱:۳۰ دقیقه یکشنبه شب (به وقت ایالات متحده)، یعنی موقعی که باراک اوباما در مورد جزییات حمله صورت گرفته سخن می‌گفت، تعداد بازدید از سایت‌های خبری به ۱/۴ میلیون عدد رسید. در همان زمان در فیس بوک صفحه‌ای - که هم اکنون نیز وجود دارد - با عنوان Osama Bin Laden is DEAD، تنها در دقایق ابتدای‌اش ۱۵۰ هزار لایک به دست آورد.» بیایید از فردی که بدون شک در پشت پرده قتل اسامه بن‌لادن حضور دارد تشکر کنیم؛ «جک بائر» و «بدون حضور بائر این اتفاق رخ نمی‌داد» از توییت‌های کاربرانی هستند که به جک بائر علاقه نشان داده‌اند. منهای تاثیراتی که مرگ بن‌لادن در شبکه‌های اجتماعی توییتر و فیس بوک گذاشت، آمار مربوط به جست‌وجو در گوگل نیز اگر چه غیرمنتظره به نظر نمی‌رسد مطمئنا قابل ملاحظه است. شرکت گوگل در کاربری توییتر خود نوشته است: جست‌وجوی عبارت «Bin Laden» در وب سایت گوگل در یکشنبه شب به میزان یک میلیون برابر افزایش یافته است. ظهور

اخباری از این دست در دنیای وب، موجب می‌شود افراد بسیاری برای دریافت اطلاعات بیشتر به سمت موتورهای جست‌وجو و شبکه‌های اجتماعی هجوم آورند و این موضوع فرصت خوبی در اختیار هکرها و سازندگان ویروس قرار می‌دهد. فاویو اسولینی، یکی از متخصصان آزمایشگاه امنیتی کسپر اسکای، در وبلاگ این شرکت نوشته است: «هکرهای مخرب بسیار سریع هستند و در چنین موقعیت‌هایی با سرعت هر چه تمام‌تر به ایجاد صفحات غیرواقعی و آلوده می‌پردازند و برخی از نتایج جست‌وجوی کنونی کاربران را به سمت صفحات مخرب هدایت می‌کنند.» این فرد متخصص برای مثال صفحه‌ای از گوگل را به اشتراک گذاشته که در آن عبارت osama bin laden body مورد جست‌وجو قرار گرفته است. زمانی که روی یکی از تصاویر کلیک کنید، به ففحه و دامین مخربی هدایت خواهید شد. - ant pe-antivirus. و /virus. cz. cc/fast-scan /cz.cc/fast-scan از این نوع صفحات مخرب هستند که به راحتی می‌توانند کامپیوتر شما را از کار بیندازند. اسولینی در ادامه می‌افزاید، هنگام جست‌وجوی تصاویر مربوط به اسامه بن‌لادن و کلا هر تصویر دیگری باید مراقب چنین ویروس‌هایی باشید. کریستن جن تایل، یکی دیگر از متخصصان کسپر در این زمینه می‌گوید: «کلاهبرداران اینترنتی، با انتخاب عبارت جست‌وجوی محبوب و استفاده از تکنیک‌های بهینه‌سازی موتورهای جست‌وجو کاربران را به دام می‌اندازند و آنها را به صفحات آلوده هدایت می‌کنند. در نهایت از آنها می‌خواهند نرم‌افزار خاصی را به عنوان آنتی ویروس یا... نصب نمایند.» این متخصص امنیتی اضافه می‌کند، صفحه جدید موجود در فیس بوک با عنوان Osama bin Laden is DEAD دارای لینک‌های تبلیغاتی است که مربوطه به برگزاری جشن قتل بن‌لادن یا ارایه بلیت و ساندویچ‌های رایگان است. با کلیک روی هر یک از این تبلیغات کاربران به صفحات مختلفی هدایت می‌شوند که از آنها اطلاعات شخصی‌شان درخواست می‌شود. این موضوع موجب می‌شود خرابکاران بتوانند به راحتی به اطلاعاتی چون ایمیل و جزییات حساس دیگر شما دسترسی پیدا کنند. برای کسب اطلاعات بیشتر در زمینه این صفحات جدید فیس‌بوک بهتر است سری به وبلاگ رسمی کسپر اسکای بزنید. آزمایشگاه سوفوس، یکی دیگر از شرکت‌های امنیتی پیشرو در این زمینه توصیه‌هایی به کاربران می‌کند: مراقب لینک‌های ارسالی در این‌باکس ایمیل و شبکه‌های اجتماعی خود باشید، لینک‌هایی که ادعا می‌کنند اخبار بیشتر و جالب‌تری در این زمینه در اختیارتان قرار می‌دهند؛ بسیاری از لینک‌های موجود در موتورهای جست‌وجو مشخصا سالم هستند و تنها برخی از آنها آلوده به ویروس هستند، بنابراین در صورتی که در مورد لینک خاصی شک دارید هرگز آن را باز نکنید.