کامپیوتر و اینترنت
اقتصادی ۲۴
پنجشنبه ۲۴ اردیبهشت ۱۳۸۸-۱۹ جمادی الاول ۱۴۳۰ -۱۴ می ۲۰۰۹ -شماره ۳۰۹۱
Thursday, 14 May 2009, Number 3091

طراحی سیستم عامل امنیتی چینی برای مقابله با آمریکا

چین اعلام کرد که یک سیستم عامل امنیتی موسوم به «Kylin» برای کامپیوترها طراحی کرده است.

به گزارش موبنا به نقل از خبرگزاری فرانسه، سیستم عامل امنیتی «Kylin» برای کامپیوترهای ارتش و دولت چین طراحی شده و امکان دسترسی آژانس‌های هوشمند و ارتش آمریکا را به کامپیوترهای دولت و ارتش چین غیر قابل نفوذ می‌کند.

این اقدام چین در نتیجه جنگ‌های سایبری با ایالات متحده آمریکا صورت گرفته است.

این سیستم عامل از سال ۲۰۰۱ تا کنون در حال طراحی توسعه بوده و تنها توسط دولت و ارتش چین مورد استفاده قرار می‌گیرد.

DELL صادرات رایانه را به کشورهای در حال توسعه ممنوع کرد

شرکت آمریکایی دل صادرات رایانه‌های از کار افتاده، مانیتور و بخش‌های دیگر را به کشورهای در حال توسعه ممنوع کرد.

به گزارش موبنا به نقل از خبرگزاری فرانسه، این اقدام شرکت دل در پی شکایت و دادخواهی سازمان حمایت از کارگران صورت گرفته است. پیش از این شرکت دل به شکل غیر رسمی و غیر قانونی به صادرات کامپیوترهای از کار افتاده به کشورهای در حال توسعه کرد که این اقدام باعث به وجود آمدن خطراتی برای کارگران و کارمندان شد. اگر چه این اعلام دل تغییر قابل توجهی را در رفتار سازندگان رایانه ایجاد نکرد اما سازمان حمایت از کارگران امیدوار است که این اقدام شرکت دل باعث ساخت استانداردهای عمومی شود. شرکت دل دیگر سازندگان دستگاه‌های الکترونیکی را مجبور به این کار خواهد کرد.

جریمه چند میلیارد دلاری اتحادیه اروپا در انتظار اینتل

انتظار می رود اتحادیه اروپا در طول نشست هفتگی کمیسرهای این اتحادیه، یکی از سنگین‌ترین جریمه‌های خود را علیه اینتل تعیین کند که امکان دارد بیش‌تر از ۳۶/۱ میلیارد دلار جریمه وضع شده علیه عملکرد ضد رقابتی مایکروسافت باشد.

به گزارش ایسنا، پرونده اینتل به شکایتی مربوط است که در سال ۲۰۰۰ از سوی AMD مطرح شده و در آن اینتل به اقدام غیرمنصفانه برای خارج کردن رقیبش از بازار متهم شد.

اتحادیه اروپا اتهامات ضد انحصارطلبی متعددی از جمله تخفیف دادن به سازندگان به شرط خرید تمام یا بخشی از پردازنده‌های اینتل، پول دادن به سازندگان برای تاخیر انداختن یا لغو خرید تراشه‌های AMD و عرضه پردازنده به زیر قیمت را مورد تحقیق قرار داد.

براساس گزارش فایننشیال تایمز، جریمه اینتل ممکن است ۱۰ درصد از درآمد سالانه جهانی اش باشد که تقریبا به ۴ میلیارد دلار بالغ می شود.

اما اینتل تنها توسط اتحادیه اروپا برای رقابت غیرمنصفانه تحت پیگرد قرار نگرفته است. کمیسیون تجارت منصفانه ژاپن در سال ۲۰۰۵ اینتل را برای سوءاستفاده از موقعیت انحصاری خود محکوم کرد. همچنین کمیسیون تجارت منصفانه کره جنوبی نیز ماه ژوئن گذشته اینتل را به دلیل تخفیف به دو سازنده رایانه کره‌ای به منظور ضربه زدن به AMD به مبلغ ۲۱ میلیون دلار جریمه دارد.

در آمریکا نیز اینتل در دادگاه فدرال در دلاور با AMD که از این شرکت شکایت ضد انحصارطلبی به عمل آورده مبارزه می کند. این شکایت که در ماه مارس ۲۰۰۵ تنظیم شده فشردگی رقابت میان اینتل و AMD را نشان می دهد که هر کدام دیگری را به تلاش برای تغییر نظرعمومی از طریق تاثیر بر رسانه‌ها متهم کرده است.

برگزاری دومین مسابقه طراحی لوگو برای گوگل

دومین مسابقه سالانه طراحی لوگوی Doodle 4 Google از سوی گوگل برگزار شده و لوگوی برنده این مسابقه به مدت یک روز در صفحه خانگی گوگل قرار خواهد گرفت.

به گزارش ایسنا، گوگل در ماه فوریه برای مسابقه طراحی لوگو برای این موتور جست و جو فراخوان داد و از دانش آموزان در آمریکا دعوت کرد در ارتباط با موضوع «چه چیزی برای دنیا آرزو می کنم؟» لوگویی طراحی کنند.

یک هیات ۱۰ نفره از داوران طرح های ارسالی را به ۴۰ فینالیست منطقه‌ای محدود کردند که به نوبه خود به چهار رده سنی کودکان سه، ۴ تا ۶ سال، ۷ تا ۹ سال و ۱۰ تا ۱۲ سال تقسیم شده‌اند.

برنده نهایی مسابقه امسال گوگل علاوه بر نمایش لوگوی طراحی شده به مدت ۲۴ ساعت در صفحه خانگی گوگل، کمک هزینه ۱۵ هزار دلاری برای مدرسه، یک لپ تاپ، سفر به اداره گوگل در نیویورک و ۲۵ هزار دلار کمک هزینه فن آوری برای مدرسه دریافت خواهد کرد.

شرکت‌های اینترنتی انگلیسی کاربران متخلف را کنترل نمی‌کنند

به تازگی انگلیس اعلام کرده که کاربران متخلف باید از سوی اپراتورهای ارائه دهنده سرویس‌های اینترنتی به شدت کنترل شوند اما ظاهرا این اقدام متوقف شده است.

به گزارش «موبنا» به نقل از پی سی ورد، شرکت‌های ارائه دهنده سرویس‌های اینترنتی در کشور انگلیس این اقدام را موجب بر انگیخته شدن خشم کاربران اعلام کردند و گفتند که چنین اقدامی را انجام نمی دهند.

این شرکت‌ها از این قضیه می ترسند که تعداد زیادی از کاربران خود را از دست داده و درآمدشان کاهش یابد. با این حال بسیاری از شرکت‌ها در پی مقابله و واکنش در مقابل افرادی که به دانلود غیر قانونی فیلم و ویدیوها می پردازند و به نوعی اقدام به نقض حقوق کپی رایت می کنند و در صدد کنترل افراد با ارائه سرعت کند دسترسی به سرویس های اینترنت یا متوقف کردن آنها هستند.

احتمال می رود در آینده قوانین و مجازات سنگین تری برای افراد متخلف در نظر گرفته شود.

اپل هم هک شد!

پس از سال‌ها، هکرها به سراغ سیستم‌های اپل آمدند و افسانه رویین تنی سیستم‌عامل مک را درهم شکستند.

هفته گذشته جان اولستیک، تحلیلگر ارشد گروه Enterprise strategy با نوشتن مطلبی راجع به امنیت سیستم‌های مک اپل روی وبلاگ خود، موجی از نظرات موافق و مخالف را به‌راه انداخت. او با استناد به گزارشی از X-Force که اوایل امسال منتشر شده بود، به این موضوع پرداخت که مک نیز نیاز به نرم‌افزارهای امنیت شبکه دارد. در گزارش X-Force که به آسیب‌پذیری سیستم‌عامل‌های رایج می‌پرداخت، سیستم‌عامل مک با ۱۴/۳ درصد آسیب‌پذیری در صدر جدول قرار داشت و پس از آن، لینوکس با ۱۰/۹ درصد، سان‌سولاریس با ۷/۳ درصد و مایکروسافت ویندوز ایکس‌پی با ۵/۵ درصد رتبه‌های بعدی را به خود اختصاص داده بودند. این وبلاگ‌نویس در گزارش خود نوشته است که سیستم‌عامل‌هایی مثل ویندوز به‌دلیل حجم بالای استفاده، دارای حفره‌های امنیتی شناخته‌شده‌ای هستند و در اکثر موارد هدف عمده هکرها هستند. اما کاربران مک به‌دلیل ناشناخته‌تر بودن نسبت به ویندوز، کمتر مورد حمله قرار می‌گیرند که این، نمی‌تواند دلیلی بر عدم استفاده از نرم‌افزارهای امنیتی برای آن‌ها باشد. اطلاعات اخیر X-Force نیز دلیل دیگری برای این موضوع است که کاربران مک نباید خودشان را ایمن تلقی کنند.

خودشان گفته‌اند

جان اولستیک در پاسخ به احساسات تند و شدید کاربران اپل نسبت به مطلب اخیرش این‌طور گفته است که خود شرکت اپل هم بارها هشدارهایی در زمینه استفاده از نرم‌افزارهای آنتی ویروس به کاربران خود داده است. نمونه بارز آن، یادداشتی بود که آذرماه گذشته در وب‌سایت این شرکت منتشر شد و کاربران را به استفاده وسیع از آنتی‌ویروس‌های چندگانه تشویق کرد. هدف اپل این بود تا ویروس‌نویسان مجبور به دست و پنجه نرم کردن با بیش از یک ابزار امنیتی شوند و پروسه تولید ویروس برای آن‌ها سخت‌تر گردد. در این وب‌سایت، ۳ نرم‌افزار مک‌آفی، سیمنتک نورتن ۱۱ و اینتگو ایکس۵ به کاربران پیشنهاد شده بود. اپل سال‌ها است که از سپری کردن دوران طلایی بدون ویروس لذت می‌برد، در حالی که ویندوز همواره آماج انواع ویروس‌ها بوده است. این رفاه‌زدگی کاربران مک را به این تصور نادرست کشانده که سیستم‌عامل آن‌ها هیچ‌گاه گرفتار ویروس نخواهد شد. اما تروژان یکی از تهدیدهای جدی مک بود. گرچه ویندوز محبوبیت بیشتری برای تروژان داشت، اما در نهایت حمله آن‌ها به مک هم آغاز شد.

به عنوان نمونه، یکی از این تروژان‌ها با نام AppleScript.THT سال گذشته به مک حمله کرد. تروژان‌ها با نفوذ به درون ماشین، به دنبال اطلاعاتی خاص می گردند و آن‌ها را برای کامپیوترهایی دیگر ارسال می کنند.

خون مک رنگین‌تر است؟

این تحلیلگر وب در پست جنجالی اش پیش‌بینی کرده بود شرکت اپل در ۱۸ ماه آینده مجبور خواهد شد کاربرانش را به استفاده از نرم‌افزارهای امنیتی اینترنت تشویق کند. همین پیش‌بینی بود که به مذاق برخی خوش نیامد. اولستیک در پاسخ به این افراد گفت: «من به هیچ وجه قصد مقایسه سیستم‌عامل مک را با ویندوز ندارم و یا نمی‌خواهم شرکت اپل را با مایکروسافت قیاس کنم. آن‌ها نباید سخنان من را حمله به اپل تلقی کنند».

او با اشاره به یادداشت وب‌سایت اپل در اول آذرماه گذشته افزود: «تمام نرم‌افزارهای پیچیده، آسیب‌پذیرند و کدهای امنیتی مک نیز از این قاعده مستثنی نیست. ویروس جدید iBotnet نمونه‌ای از این حملات خطرناک است و احساس من این است که حملات ویروس‌ها به مک در سال آینده شتاب بیشتری خواهند گرفت». جان اولستیک معتقد است هک کردن مک، کار بسیار آسانی است. او به مسابقه‌ای که اسفندماه برگزار شد، اشاره کرد که در آن چارلی میلر که متخصص امنیت شبکه است، توانست در کمتر از ۱۰ ثانیه یک حفره امنیتی را در مک شناسایی کند. او افزود: «اگر میلر توانست در ۱۰ ثانیه این کار را انجام دهد، پس دیگران می‌توانند در یک ساعت به مک نفوذ کنند و این همان فکری است که من را می‌ترساند».

با تمام این اوصاف بد نیست شرکت اپل هم دست از لج‌بازی بردارد و به کاربرانش جدا توصیه کند از نرم‌افزارهای امنیتی استفاده کنند. هدف اصلی کاهش خطرات احتمالی است.

kabaronline.ir

کلوچه های خوشمزه!

تقریبا تمام سایت‌هایی که بازدید می کنید اطلاعاتی را در قالب یک فایل کوچک متنی (Text) بر روی کامپیوتر شما ذخیره می کنند به این فایل کوکی می گویند مثل ذخیره شدن این فایل در فولدر Temporary Internet Files در اینترنت اکسپولرر و در نت اسکیپ در فولدر Cashe است در اپرا و موزیلا و نسخه‌های قدیمی تر اینترنت اکسپولرر در فولدر جدایی به نام کوکی است.

انواع مختلفی از کوکی ها وجود دارد و شما در نسخه‌های جدیدتر وب بروسرها (Web Browsers) این امکان را دارید که انتخاب کنید کدام کوکی‌ها برروی کامپیوتر شما ذخیره شوند در صورتی که کوکی ها را کاملا غیر فعال کنید ممکن است بعضی سایت‌های اینترنتی را نتوانید ببینید و یا از بعضی امکانات مثل به یاد داشتن شناسه و رمز عبور شما در آن سایت محروم شوید و یا انتخاب‌هایی که داشتید مثل ساعت محلی و یا دمای هوای محلی و کلا از تنظیمات شخصی‌ای که در آن وب سایت انجام داده اید نتوانید استفاده کنید.

کوکی ها چگونه مورد استفاده قرار می گیرند؟

همانطوری که گفتیم کوکی یک فایل است که توسط یک وب سایت برای حفظ اطلاعات بر روی کامپیوتر شما قرار می گیرد یک کوکی می تواند شامل اطلاعاتی باشد که شما در آن سایت وارد کرده اید مانندای میل - آدرس - شماره تلفن و سایر اطلاعات شخصی - همچنین کوکی ها می توانند صفحات و یا کارهایی را که در آن وب سایت انجام داده اید مثل تعداد کلیک لینک‌های بازدید شده و مدت بازدیدرا نیز ضبط کنند. این به سایت کمک می کند تا دفعه بعد که به آن سایت بازگشتید اطلاعات شما را به خاطر داشته باشد و از وارد کردن تکراری اطلاعات خودداری کنید نمونه بارز این مطلب لاگ این ماندن شما در آن سایت است و یا پیغام‌های Welcome Back و یا حفظ تنظیماتی که درآن سایت انجام داده این به عنوان مثال می توان به خصوصی کردن صفحه My MSN اشاره کرد. نکته‌ای را که باید به خاطر داشته باشید این است که هر وب سایت فقط می تواند از اطلاعاتی که شما وارد کرده اید استفاده کند نه بیشتر مثلا اگر ای میل خود را در آن سایت وارد نکرده اید آن وب سایت نمی تواندای میل شما را به دست آورد و یا به سایر اطلاعات کامپیوتر شما دست یابد. مورد دیگر اینکه وب سایت‌ها فقط می‌توانند کوکی‌هایی را که خود ایجاد کرده اند بخوانند و نمی‌توانند از سایر کوکی‌های موجود استفاده کنند. وقتی که از یک وب سایت برای بار دوم بازدید می‌کنید آن وب سایت به دنبال کوکی مربوط به خود می گردد و در صورت وجود از آن استفاده می کند. (البته باز هم با توجه به تنظیماتی که انجام داده اید)

انواع کوکی ها:

کوکی‌های پایا - دائمی (presistent Cookies):

این نوع کوکی‌ها به عنوان یک فایل بر روی کامپیوتر شما ذخیره می‌شوند و بعد از بستن مرورگر اینترنتی شما پاک نخواهند شد و همچنان باقی می‌مانند. این کوکی‌ها قابلیت به روز شدن توسط سایت ایجاد کننده خود را دارند همچنین سایت اجازه دسترسی مستقیم به این کوکی‌ها را نیز دارد حدود ۸۰ درصد کوکی‌های مورد استفاده از این نوع هستند.

کوکی‌های موقت (Temporary Cookies):

کوکی‌هایی هستند که بعد از بستن مرورگر اینترنتی شما و یا خروج از سایت استفاده کننده از کوکی پاک می‌شوند.

نوع دیگر کوکی‌های موقت کوکی‌های زمان دار هستند که زمانی برای کار دارند و بعد از آن اصطلاحا Expire می‌شوند و از کار می‌افتند ولی پاک نمی‌شوند و در صورت بازدید مجدد از سایت ممکن است به روز رسانی شوند و مجددا مورد استفاده قرار بگیرند.

کوکی‌های ناخوشایند (Unsatisfactory cookies):

این کوکی‌ها اجازه دسترسی به اطلاعات خصوصی شما را برای استفاده دوباره بدون پرسیدن از شما دارند از این کوکی‌ها بیشتر در خریدهای اینترنتی و سایت امن (SSL) مورد استفاده قرار می‌گیرند.

مقایسه کوکی‌های متعلق به سایت اصلی (First Party) و کوکی‌های متعلق به سایت‌های دیگر (Third Party):

قبل از هر چیز با دو مفهوم First& third party اشنا می‌شویم این مفاهیم در حقیقت مفاهیم بیمه‌ای هستند:

First Party: عضو اصلی یک خانواده و یا شرکت صاحب حقوق و مزایای اصلی کسی که بیمه نامه اصلی را داراست(Policy Holder)

Second party: شرکت بیمه کننده

Third Party: هر شخص سومی غیر از این دو

و اما این مفاهیم در کوکی‌ها چه معنایی می‌دهند؟

First Party: کوکی‌هایی هستند که فقط اطلاعات آنها به سایت که توسط آنها ایجاد شده اند فرستاده می‌شود و کار آنها همانطور که اشاره شد یادآوری اطلاعات ماست.

Third Party: کوکی‌هایی هستند که اطلاعات را به چندین سایت مختلف غیر از آنچه بازدید می‌کنید می‌فرستند استفاده این کوکی‌ها معمولا تجاری است بدینگونه که شما از سایتی بازدید می‌کنید و آن سایت دارای بنرهای تجاری و تبلیغات از سایت دیگری (Third Party) می‌باشد در اینجاست که کوکی Third Party وارد عمل شده و اطلاعات شما را ثبت می‌کند به عنوان مثال صاحب تبلیغ با استفاده از این امکان می‌تواند ببیند که شما چه نوع تبلیغ‌هایی را بازدید می‌کنید و در کدام سایت ها. این نوع کوکی هم می‌توانند از نوع دائمی و هم موقت باشند. اصولا این نوع کوکی‌ها استاندارد نیستند و توسط مرورگرهای جدید بلوک می‌شوند. همچنین این کوکی‌ها ممکن است به هکرها کمک کنند تا اطلاعات شخصی شما را بدست بیاورند. (برای جلوگیری از آخرین پچ‌های مرورگر خود استفاده کنید) اصولا پیشنهاد می‌شود تا این کوکی‌ها را که هیچ استفاده مفیدی برای کاربر ندارند بلوک کنید.

هدف اصلی کوکی‌ها شناسایی کاربران است تا تنظیماتی را که کاربر بنا بر سلیقه خود دفعه قبل روی یک وب سایت مثلا یاهو انجام داده اکنون هم بتواند صفحه را با همان تنظیمات دفعه قبل برایش باز کند. برای مثال فرض کنید در Hotmail یک ایمیل درست کرده اید و اکنون بعد از چند روز دوباره وارد سایت Hotmail می‌شوید تا با وارد کردن ID (یا شناسه) و پسورد وارد ایمیل خود شوید و مشاهده می‌کنید که با باز شدن صفحه ID شما از قبل نوشته شده است یا حتی اگر از قبل این امکان را ایجاد کرده باشید پسورد شما هم وارد شده فقط کافیست اینتر را بزنید و وارد ایمیل خود شوید. و زمانیکه در گوگل زبان خود را انتخاب می‌کنید و دفعه بعد که وارد گوگل می‌شوید و زبان مورد نظر شما به طور اتوماتیک انتخاب شده است همه این کارها و بسیاری از کارهای دیگر اینچنینی بوسیله کوکی‌ها انجام می‌شود در حقیقت از طریق کوکی‌ها سرور وب صفحات را مطابق عادت و سلیقه شما باز می‌کند و به این طریق در وقت و حوصله شما صرفه جویی می‌شود.

مشکلات کوکی‌ها

کوکی‌ها مکانیزم کاملی برای شناسایی نیستند، ولی کارهایی را ممکن می‌سازند که شاید بدون آنها انجام همین کارهای ساده غیر ممکن بود. در اینجا به بررسی چند مشکل که از کارایی کوکی‌ها می‌کاهد می‌پردازیم.

افراد معمولا از کامپیوترها به طور مشترک استفاده می‌کنند. هر کامپیوتری که در یک مکان عمومی مانند محل کار یا حتی در خانه معمولا به طور اشتراکی چند نفر از آن استفاده می‌کنند. و چندین نفر در زمان‌های مختلف بوسیله این کامپیوتر به اینترنت متصل می‌شوند. کوکی‌ها نمی‌توانند نیاز همه آنها را همزمان برآورده کنند. فرض کنید از یک مکان عمومی مانند یک کافی نت در حال خرید از یک فروشگاه اینترنتی هستید. این فروشگاه اینترنتی روی کامپیوتری که از آن برای خرید استفاده می‌کنید یک کوکی قرار می‌دهد تا اگر بار دیگر وارد این فروشگاه اینترنتی شدید حساب شما را استفاده کند. فروشگاههای اینترنتی معمولا در این زمینه بسیار هشدار می‌دهند. یا فرض کنید که شما با استفاده از کامپیوتر شخصی همسرتان از فروشگاه اینترنتی آمازون خرید کرده اید و حال اگر همسرتان بعد از شما برای خرید وارد آمازون شود فقط با یک کلیک می‌تواند خرید کند البته با حساب شما!

در یک کامپیوتر با سیستم عاملی مانند ویندوز NT یا یونیکس که حسابها به طور مناسب و درست در اختیار کاربران قرار می‌گیرند کمتر این مشکلات پدید می‌آیند.

اگر کوکی‌ها پاک شوند. اگر شما با مرورگر خود (مانند اینترنت اکسپلورر) مشکل دارید و از شرکت پشتیبانی کننده این مرورگر کمک بخواهید ممکن است اولین چیزی که به شما بگویند تا انجام دهید پاک کردن temporary Internet files یا همان فایلهای موقت اینترنتی در شاخه ویندوز باشد. زمانیکه این کار را می‌کنید تمام کوکی‌ها را از دست می‌دهید و اگر سایتی را که قبلابازدید کرده اید بعد از این عمل دوباره بازدید کنید آن سایت شما را به عنوان یک کاربر جدید فرض خواهد کرد و برای شما یک کوکی جدید می‌فرستد. و به همین علت است که بعضی از سایتها از شما می‌خواهند که در آنها ثبت نام کنید (یا اصطلاحا رجیستر شوید.) جون اگر با یک کلمه کاربری (User Name) و یک کلمه عبور (Password) شما می‌توانید وارد حوزه شخصی خود در آن سایت شوید حتی اگر فایل کوکی را از دست داده باشید.

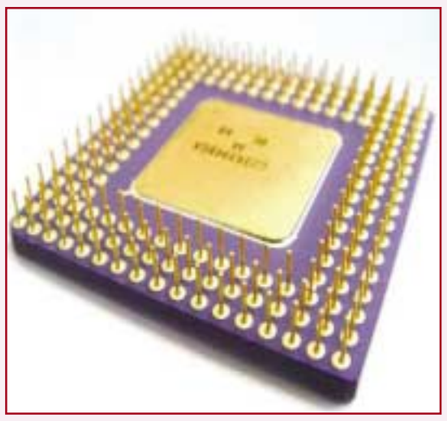
افراد زیادی در روز از بیش از یک کامپیوتر برای دستیابی به اینترنت استفاده می‌کنند. به عنوان مثال اگر شما یک کامپیوتر در محل کار و یک کامپیوتر در خانه و یک لپ تاپ برای خارج از این دو محل استفاده می‌کنید برای هر کامپیوتری که با آن به یک وب سایت متصل می‌شوید کوکی‌های جداگانه برای هر کامپیوتر ارسال می‌شود و این سبب می‌شود که تنظیمات خود را برای هر کامپیوتر به طور جداگانه انجام دهید که خسته کننده است.

حل مشکلات مذکور احتمالا به همین سادگی‌ها هم نیست مگر اینکه از کاربر خواسته شود در سایت مذکور ثبت نام کند.

daneshema.com

کد FCC چیست؟

اگر تا به حال با قطعات سخت افزار کامپیوتر سر و کار داشته اید احتمالا متوجه شده اید که بسیاری از قطعات بدون مارک به نظر می‌رسند و در بسیاری موارد قطعات بوسیله



همان کارخانه‌ای که نام آنها روی قطعه حک شده، ساخته نشده است. بلکه در کارخانه‌ای در تایوان یا چین ساخته شده است. مثلا کارت صدایی با مارک یاماها فقط چیپ آن توسط این کارخانه ساخته شده است. ولی خود کارت ممکن است در چندین کارخانه دیگر ساخته شود.

اما برای دانلود نرم‌افزار یک قطعه باید دریافت سازنده واقعی قطعه کیست تا درایور آن را بدست آورد.

آنچه در این مقاله می‌خواهیم در مورد آن صحبت کنیم کد FCC است که روی بسیاری قطعات سخت افزاری قابل مشاهده است. هر قطعه سخت افزاری یا الکترونیکی یک کد FCC دارد. این کد یک کد شناسایی ثبت شده در FCC (مخفف Federal Communication Commission) است، در محلی قابل دید روی قطعه پرینت می‌شود. با استفاده از این کد می‌توانید اطلاعات زیادی در مورد قطعه مورد نظر خود بدست آورید.

دقت کنید که ممکن است بعضی از قطعات دارای ۲ کد FCC باشند یکی را FCC ID و یکی را FCC REG گویند. و برای جستجوی اطلاعات در مورد قطعه مورد نظر باید کد FCC ID مد نظر قرار گیرد.

فرض کنید کد FCC یک قطعه HBQDM336P_DFV1 باشد در این کد سه حرف اول یعنی HBQ اطلاعات مربوط به نام تجاری کارخانه سازنده را می‌دهد ولی اگر کد را به صورت کامل وارد کنید اطلاعات دقیق تری بدست می‌آورید. مثلا متوجه خواهید شد که کد بالا مربوط به یک مودم است و . . .

yabegir.com

مایکروسافت:

هکرها به کاربران پاورپوینت حمله می‌کنند

شرکت مایکروسافت به کاربران برنامه پاورپوینت در مورد حمله هکرها هشدار داد.

به گزارش موبنا به نقل از خبرگزاری فرانسه، هکرها در حال حاضر در جستجو برای حمله به نرم‌افزار پاورپوینت کامپیوترهایی که به ویندوز مجهزند هستند و مایکروسافت در اقدام به مقابله با حمله هکرها یک وصله نرم افزاری ارائه کرد.

سازنده شماره یک نرم‌افزار جهان می گوید نسخه پاورپوینت را برای کامپیوترهای مک اپل نیز ارائه کرده که این مدل کامپیوترها نیز در مقابل حمله هکرها نفوذ پذیر شده اند.

البته مایکروسافت اعلام کرد که هنوز هیچ مدرکی مبنی بر اینکه هکرها به این نرم افزارها دست پیدا کرده اند نیافته است. بر این اساس در رابطه با هشدار به کاربران بیانیه‌ای فرستاد که هکرها در حال جستجو برای دستیابی به نفوذ پذیری در پاورپوینت هستند که تمایل به قربانی و آلوده کردن فایل های پاورپوینت دارند.

بر این اساس کاربران لازم است وصله امنیتی مایکروسافت را یا خود از وب سایت این شرکت دانلود کنند یا به شکل ایمیل دریافت کنند.