آموزش نصب گوگل گروم از طریق شبکه با گروپ پالیسی قسمت ۳ (نسخه PDF)

در بخش سوم مقاله آموزشی انتشار و امن سازی گوگل کروم به مباحثی از قبیل plugin ها ، java script و ... خواهیم پرداخت

JavaScript

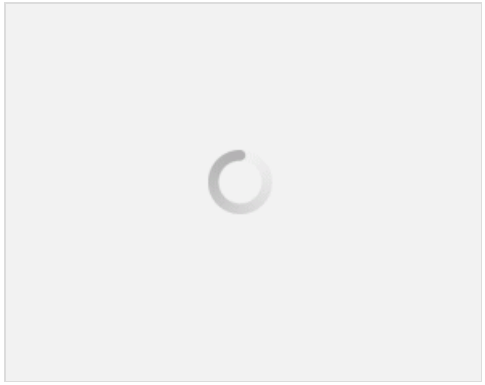
همانطور که مطلع هستید JavaScript نقش بسـزا و در برخی مواقع پـایه ای در اکثر وب سایتها و بهبود عملکرد کاربران دارد ولیکن گوگل کروم این قابلیت را دارا می باشد که بر اساس سـیاست های شما از کارکردن اسکریپت های جاوا ممانعت به عمل آورد و این امر به منظور به دست آوردن امنیت بیشتر می باشـد و لیکن محدودیتهای بسـیاری هم در پی دارد . اکثر کاربران برای مشاهده کامل وب سایتها نیاز به دسترسی کامل به جاوا اسکریپت دارند که این امر در ابتدا با محدود نمودن اجرا کامل جاوا اسکریپت و پس از آن ایجاد یک لیست سفید و تعریف دومین های مورد تائید در آن امکان پذیر خواهد بود .

این راهکار جزء راهکارهای خوب security practice بوده که امنیت شـبکه و کاربران را می توان به وسـیله آن تضمین نمود ولیکن این امر باعث بروز ترافیک کاری بیشتری برای مـدیران شـبکه خواهـد شـد چرا که با درخواست های بیشـماری از سوی کاربران شـبکه در خصوص تخصـیص مجوز اسـتفاده از وب سایت مورد علاقه خود روبرو خواهنـد شد که در صورت تائید می بایست در لیست سـفید ایجاد شد درج شوند .

مثال زیر درخصوص همین مسئله در مسیر

\Google\Google Chrome\Content \Settings

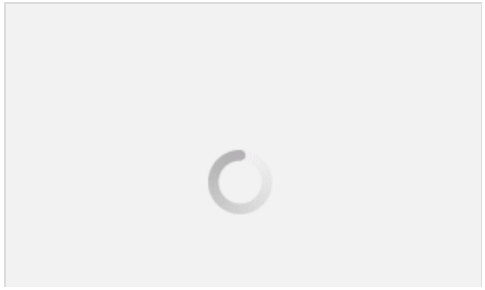
با نحوه تنظیمات Allow Javascript on these sites و Block Javascript on these sites بوده که به دومین های gov و mil مجوز استفاده از اسکریپ ت های جاوا داده شده و مابقی دومین ها این مجوز را نخواهند داشت



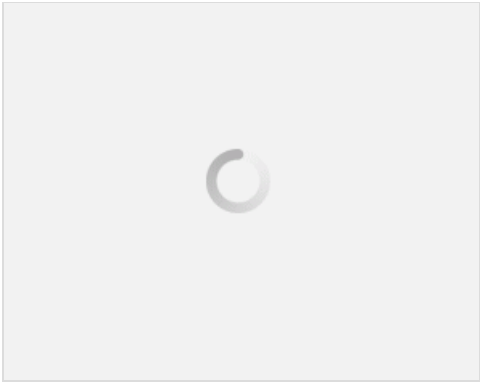
Plugins

ساختار و معماری کروم برای نمایش محتویات سایت ها بر اساس استفاده از پلاگین ها می باشد که بسته به مکان و موقعیت با اجرا نمی شوند Chrome sandbox افزودن پلاگین ها می توان از آنها بهره جست اکثر پلاگین ها در

مجوز اجرای خودسـرانه پلاگین ها علاوه بر افزایش بار بر روی کروم و شـبکه باعث ایجاد بستری جهت حملات اینترنتی به دسـتگاه شـما خواهد شد. در نصب کروم چندین پلاگین موجود است که می بایست به صورت پیش فرض فعال و نصب شود که شرح آنها در جدول زیر آورده شده است .



ایجاد لیست سـیاه و درج تمامی پلاگین ها در آن و تعریف لیست سـفیدی از پلاگین ها اکیـدا توصـیه می شود انجام این مهم با تعریف مقدار * برای پالیسـی Specify a list of disabled plugins و پس از آن تعریف پلاـگین های جدیـد در Specify a list of enabled plugins صورت می پذیرد لیست سفید از اجرای پلاگین های فاقد مجوز جلوگیری میکند .



جـداول فوق ریسک هایی که با فعال سازی پلاگین ها ی فعال شـده را نمایش می دهـد . اگر پلاگین های شـما از پلاگین های ((NPAPI Netscape Plugin Application Programming Interface استفاده کند در آنصورت آن یک sandboxed نخواهد بود و در صورتیکه از (، (PPAPI Pepper Plugin Application Programming Interface استفاده کند می تواند sandboxed باشد .

در حـالت کلی پلاگین های Sandboxed می بـایست همیشه بر یک non-sandboxed plugins اجرا شود.البته در جـداول فوق پلاگین های استفاده شده اکثراً sandboxed نمی باشند .

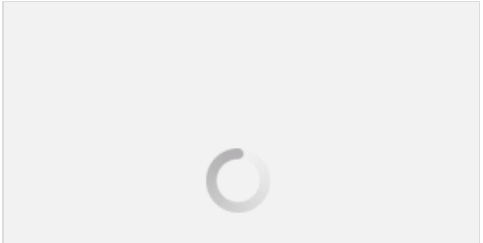
کروم پشتیبانی خود را از sandboxed نرم افزارهای Adobe Flash و Adobe PDF reader رو از نسخ ۸ و ۲۱ آغاز کرد البته در نظر بگیرید که از ویندوز ۸ پلاگین هایی که NPAPI نباشند قابلیت اجرا دارند .

یک مدیر شبکه می تواند با نگاه به آدرس chrome://plugins در کروم Omnibox از پلاگین های موجود در کروم اطلاع حاصل نماید همچنین بـا کلیک بر روی گزینه Details در سـمت راست به جزئیـات پلاگین ها ماننـد نوع NPAPI یا PPAPI ، نـام ، محـل و ... دست پیدا نمایند .مدیران شبکه در جریان باشند برای اینکه لیست سفید آنها به درستی کار کند می بایست دقیقا نام پلاگینی که در قسمت جزئیات نمایش داده شده را در لیست سـفید درج نمایند حساسـیت به حروف بزرگ و کوچک وجود دارد همچنین لیست سـفید از کرترهای عمومی و ؟ **نیز پشتیبانی می نماید به طور مثال عبارت** QuickTime Plug-in یا ?.?.? QuickTime Plug-in به معنی مجوز اجرای کلیه نسخ پلاگین های QuickTime می باشد همچنین **Microsoft Office** به معنی استفاده از پلاگین های Microsoft Office می باشد البته برخی محصولات مانند Java و RealPlayer جهت اجرا نیاز به نصب پلاگین های مختلفی دارنـد در واقع لیست سـفید پلاگین ها می تواند شامل URL های باشـد که مجوز اجرای پلاگین هایشان را دارنـد به طور مثال شـما می توانید اجرای پلاگین Adobe Flash را جهت وب سـایت های خاص فعال سازید.

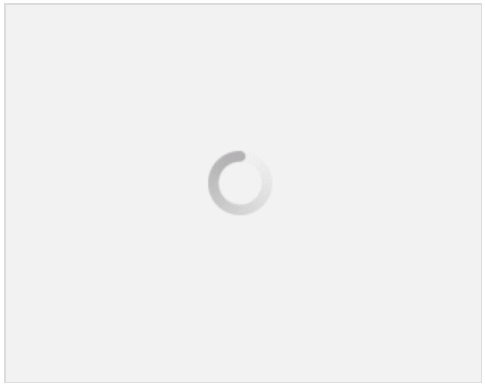
شکل نمایش داده شده زیر نحوه تنظیمات این مهم نشان داده شده است که در مسیر

\Google\Google Chrome\Content Settings

و Block Plugins on these sites می باشد و با فعال سازی گزینه Plugins on these sites در جهت بلاک کردن کلیه پلاگین ها به جز دامین .gov و .mil این مهم صورت می پذیرد مدیران شـبکه می توانند گزینه further restrict plugins را به منظور اجرای پلاـگین ها فقط بر روی ارتباطات HTTPS انتخاب نمایند و زمانیکه این آیتم انتخاب می شود بر سایر پالیسی ها ارجحیت می یابد .



یکی از راه های جلوگیری از exploited کاربران شـبکه جلوگیری از اجرای پلاگین های منقضی شده می باشد که این آیتم با Disabled کردن گزینه Allow running plugins that are outdated می باشـد در شـکل زیر نمایشـی است از آنچه که کـاربران در زمـان فعـال بودن گزینه بالا خواهند دید آورده شده است :



که در این حالت مدیر شبکه با مراجعه به chrome://plugins و دیدن جزئیات پلاگین منقضی شده به نسبت به دانلود لینک

Download Critical Security Update

جهت رفع مشکل اقدام نمایند .

بخش چهارم مقاله ما در خصوص ارائه توضیحاتی در خصوص Google Update ، Extensions و Appendix خواهد بود .

نویسنده : رضا صاحبی

منبع : انجمن تخصصي فناوری اطلاعات ایران

#Publish_کردن_نرم_افزارها_در_شبکه #شبکه_و_زیرساخت

علی نخعی
با سلام جناب صاحبی و تشکر از مقاله خوب شما
با توجه به اشـکالات دسـتوری که به نظر در متن وجود دارد لطفا متن را یک باز بینی و اصلاح بفرمایید چون برخی قسمتهای آن مبهم میباشد

مطلب اصلی