بسم الله الرحمن الرحيم

{ الحماية من تسريبات المتصفح }

الحمدلله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد

كما ننوه دائما ان الحماية عملية معقدة لا تعتمد علي اداة او برنامج وتعتمد بشكل كبير علي الوعي الامني لدي الانصار فهذا الدرس هام جدا لجميع الانصار بلا استثناء نظرا لان معظمهم يستخدمون متصفحات تسرب عناوين الIP الخاصه بهم رغم استخدامهم للشبكات الخاصة الافتراضية (VPN)

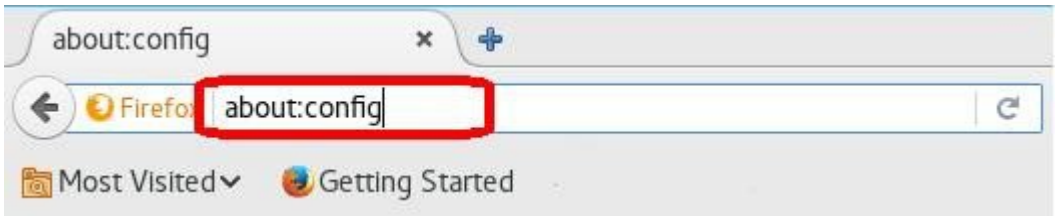
WEB RTC : بروتوكول اتصالات جديد يعتمد علي الجافا سكريبت حيث يمكنه تسريب عنوان الIP الخاص بك اثناء استخدامك للشبكات الخاصة الافتراضية (VPN)

إضافة NO Script تمنع تسريب البروتوكول لكن احيانا تتعطل اضافات المتصفح فالافضل غلق البروتوكول يدويا من اعدادات المتصفح

أولا : افحص اتصالك بهذا الموقع Ipleak.net

إن ظهر عنوان الIP الخاص بك اسفل خيار WEB RTC Detection فهذا يعني ان بروتوكول WEB RTC يعمل

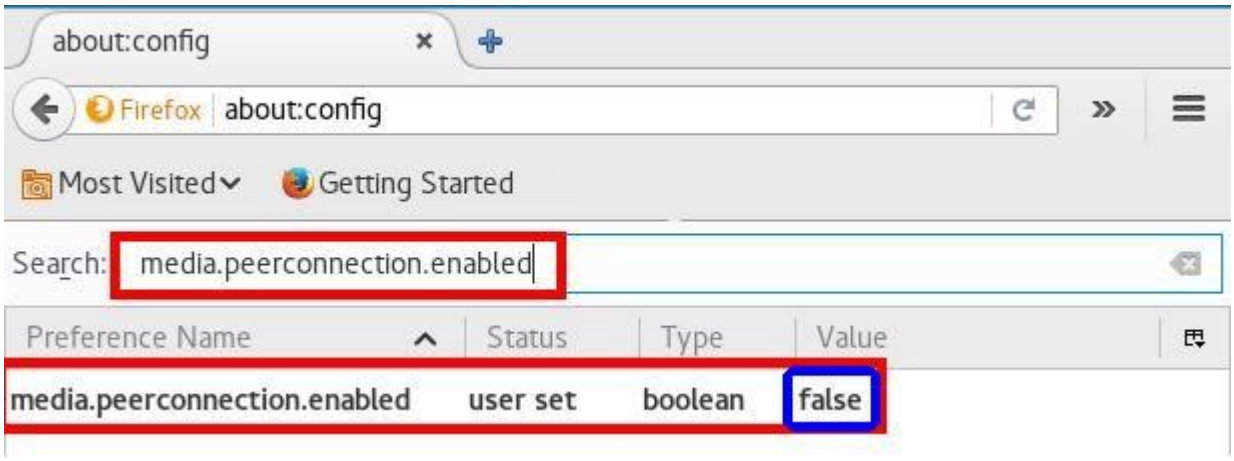
كيف اعطل بروتوكول WEB RTC في متصفح FIREFOX



إفتح متصفح Firefox ثم اكتب هذه الجملة في المكان الموضح بالصورة

about:config

إضغط علي I'll be careful , I promise



ستظهر لك قائمة طويلة وبالاعلي نافذة صغيرة للبحث انسخ هذه الجملة media.peerconnection.enabled والصقها في نافذة البحث

سيظهر لك الخيار بالاسفل اضغط عليه مرتين حتي تتحول قيمة البروتوكول من True الي False

بعد ذالك افحص اتصالك مجددا بموقع Ipleak.net

ان لم يظهر عنوان الIP الخاص بك كما موضح في الصورة فهكذا لا يوجد تسريب من بروتوكول WEB RTC

- اذا اردت التحقق من ان كل خيار متعلق ببروتوكول WEB RTC معطل فافعل الاتي:

- ابحث عن media.peerconnection.turn.disable وتحقق ان قيمته True

- ابحث عن media.peerconnection.use_document_iceservers وتحقق ان قيمته False

- ابحث عن media.peerconnection.video.enabled وتحقق ان قيمته False

- ابحث عن media.peerconnection.identity.timeout وتحقق ان قيمته 1

ـــ الان انت امن بنسبة 100% من تسريب بروتوكول WEB RTC لعنوان الIP الخاص بك ـــ

ماذا عن المتصفحات الاخري ؟

O متصفح Tor او Orfox باندرويد لا يحتويان علي بروتوكول WEB RTC

O متصفح جوجل كروم متوفر له اضافة Web Rtc Block لكنها لا تعمل بكفاءة فالافضل استخدام متصفح Firefox كبديل

O متصفح Safari علي نظام Ios لا يحتوي علي بروتوكول WEB RTC

لكن ننصح باستخدام Firefox بدلا عنه

دروس أمنية

- دورة أمن الهواتف الذكية
- دورة احتراف لينكس منت
- الحرب الالكترونية وغفلة أنصار الدولة الاسلامية
- وداعا لجوجل وياهو ومرحبا بالبريد الالكتروني المشفر
- Smartphone Security
- تايلز افضل وأأمن نظام تشغيل
- الارشيف التقني
- خدمات الVPN

كتبه خادم الموحدين : تقني الدولة الاسلامية

استكمال لشرح منع تسريب رقم ip سنقوم الان بشرح إيقاف تسريبات سيرفرات DNS وفي البداية علينا معرفة ماهو الـ DNS؟

سيرفر الـDNS يحول الموقع من العنوان الحرفي الى عنوان رقم بمعنى انك اذا طلبت موقع www.EX.com فإن المتصفح لا يفهم هذا فيحول الطلب لسيرفر DNS ليتم تحويل الرابط الى ارقام وهي اللغة التي يفهمها المتصفح

1- للكشف عن تسريبات DNS ادخل هذا الموقع
/http://www.dnsleaktest.com

2- اذا وجدت علم البلاد التي تقيم فيها فهذا يعني وجود تسريب يكشف هويتك

3- اذهب الى أبدا ثم تشغيل ثم اكتب cmd ثم انتر

4- اكتب هذا الامر ipconfig /flushdns ثم انتر لمسح الذاكرة الموقتة

5- الان سنغيّر سيرفرات DNS بفتح خصائص الشبكة ثم الكبس على اسم شبكتك ثم خصائص

6- ومن ثم اختر nternet Protocol Version 4 TCP/IPv4 قم استخدام سيرفر DNS

7- استخدم هذا السيرفر وهو من شركة open DNS وهو عام وغير مشفر | Open DNS: 208.67.220.220 , 208.67.222.222

8- أعد الفحص ولن تجد تسريب ان شاء اللّه