



معلومات الكاتب

الكاتب : ezat

المنتدى : [شبكة منتديات الرقة](#)

البريد : raqqanetworks@gmail.com

البلد : سوريا - الرقة

محرر نهج المجموعة المحلي "اعدادات النظام المتقدمة"

local Group Policy Editor

شرح بالصور لطريقة

التخلص من اضرار الفيروسات في النظام واصلاحها

بسم الله الرحمن الرحيم

مقدمة:

محرف نهج المجموعة المحلي للكمبيوتر هي الاعدادات المقدمة للنظام مثل :
السماح للمستخدم بالوصول الى **محرف الرجستري** أو السماح بالوصول الى
أدارة المهام.....الخ

والتي تقوم الفيروسات بإيقافها بأمر واحد وبسرعة وبطريقة مختصرة .

الآن كيف يمكن تشغيل **الرجيستري** او **ادارة المهام** او **موجه الاوامر... اذا تم**
ايقافه من قبل فيروس !

نبدأ على بركة الله

كيف نصل الى محرف نهج المجموعة المحلي ؟

على نظام

Win xp

ندخل

أبدأ - تشغيل

ونكتب الامر

Gpedit.msc

موافق

أما في نظام win7

أبدأ - كافة البرامج - البرامج الملحقة - تشغيل

ونضع نفس الامر

Gpedit.msc

موافق

** بإمكانك نسخ الامر ولصقه **

كما في الصورة :



شبكة ومتمديات الرقة

ملاحظة : لتسهيل حفظنا الامر `gpedit.msc` نقوم بتحليله ومعرفة معناه

هي اختصار لـ **Group Policy Editor** أي محرر نهج المجموعة

حيث حرف **g** هو اختصار لـ **group** اي مجموعة

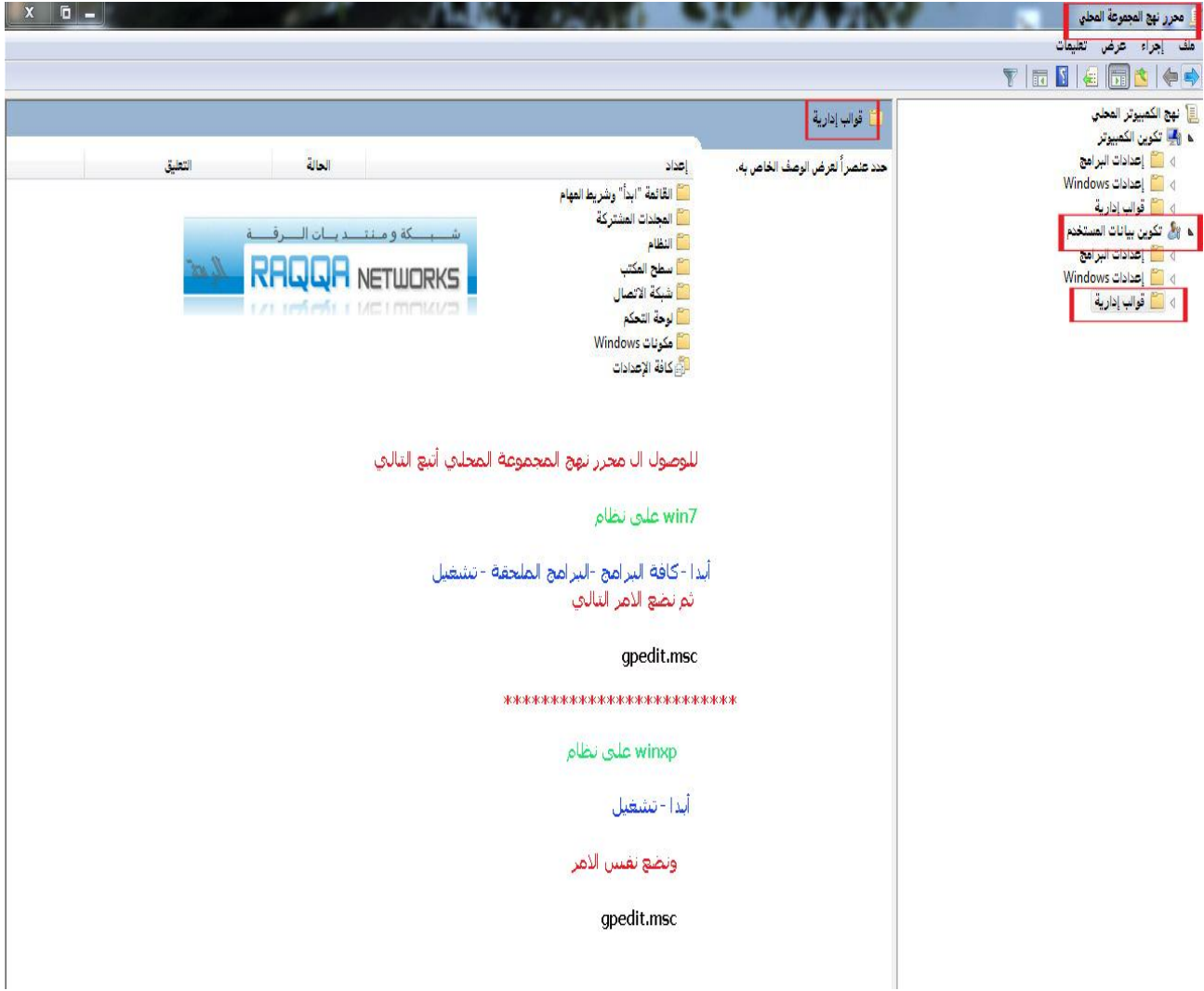
وحرف **p** هو اختصار لـ **policy** أي نهج

و **Edit** هو اختصار لـ **Editor** أي محرر

أما **msc** هي لاحقة البرنامج مثل **exe** و **swf**.....الخ و لا تنسى وضع نقطة (.)

ملاحظة : البرنامج في كل الانظمة مثبت تلقائيا .

الآن نتعرف على واجهة محرر نهج المجموعة المحلي



صورة توضح محرر نهج المجموعة المحلي

طبعا الذي يهمنا القسم :

* تكوين بيانات المستخدم *

الان بعد كل هذا الشرح المطوّل لطريقة الوصول الى محرر نهج المجموعة

نبدأ العمل !

1 - حل مشكلة تم تعطيل الرجستري من قبل المسؤول

الرجيستيري مهم جدا في تسجيل البرامج أو الالعب... الخ في النظام .

يقوم الفيروس عند دخوله الى جهازك بتعطيل الرجيستيري وهو لا يقوم بحذف برنامج الرجيستيري كما يعتقد البعض بل يقوم بإيقافه من **محرف نهج المجموعة**

كالتالي:

منع الوصول الى ادوات تحرير الرجيستيري

فيختار الفيروس : ممكن

ونحن سنقوم بالتعديل الى : معطل

أو : غير مكون

لكي نستطيع تشغيل الرجيستيري.

حل المشكلة :

نقوم بالدخول الى محرف المجموعة المحلي (شرحت طريقة الوصول الى المحرف في الاعلى)

بالأمر `gpedit.msc`

وندخل كالتالي :

١- محرف نهج الكمبيوتر المحلي ٢- تكوين بيانات المستخدم ٣- قوالب ادارية ٤ - النظام

٥- منع الوصول الى ادوات محرف الرجيستيري

ونضغط عليه نقرتين :ونختار

معطل أو غير مكون أي تلقائي

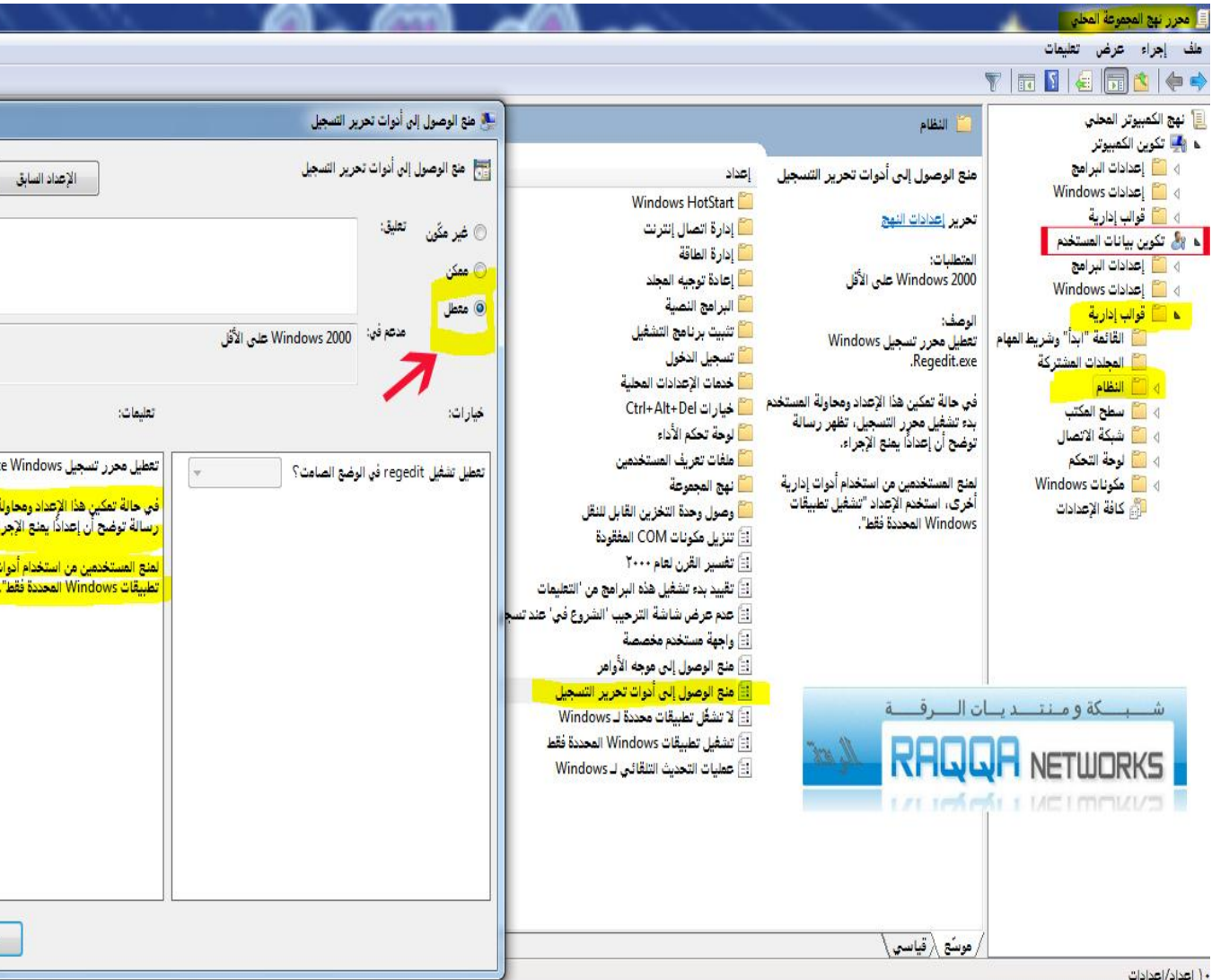
ثم

موافق

ويتم تشغيل الرجيستيري

شرح بالصور لطريقة تشغيل الرجيستيري :

.....



صورة تبيّن طريقة تشغيل الريجستري

٢- حل مشكلة تم إيقاف ادارة المهام من قبل المسؤول أو **ctrl+alt+delete**

Taskmanegar

ادارة المهام

مهم جدا في مراقب العمليات التي تعمل في الخلفية وأنهاء البرامج التي لا تستجيبالخ

"مثل الريجستري"

يقوم الفيروس بمنع المستخدم من الوصول الى ادارة المهام

(لا تنسى عن طريق محرر المجموعة المحلي)

الامر

gpedit.msc

****أنسخ الامر واللصقه****

كالتالي:

خيارات **ctrl+alt+delete**

ثم

ازالة ادارة المهام

الفيروس يعمل: ممكن

ونحن نعمل: معطل أو غير مكون

حل المشكلة:

ندخل :

محرر نهج المجموعة المحلي

+

تكوين بيانات المستخدم + قوالب ادارية + النظام + خيارات **ctrl+alt+delete** **ننقر عليها مرتين**

فتظهر

ازالة ادارة المهام

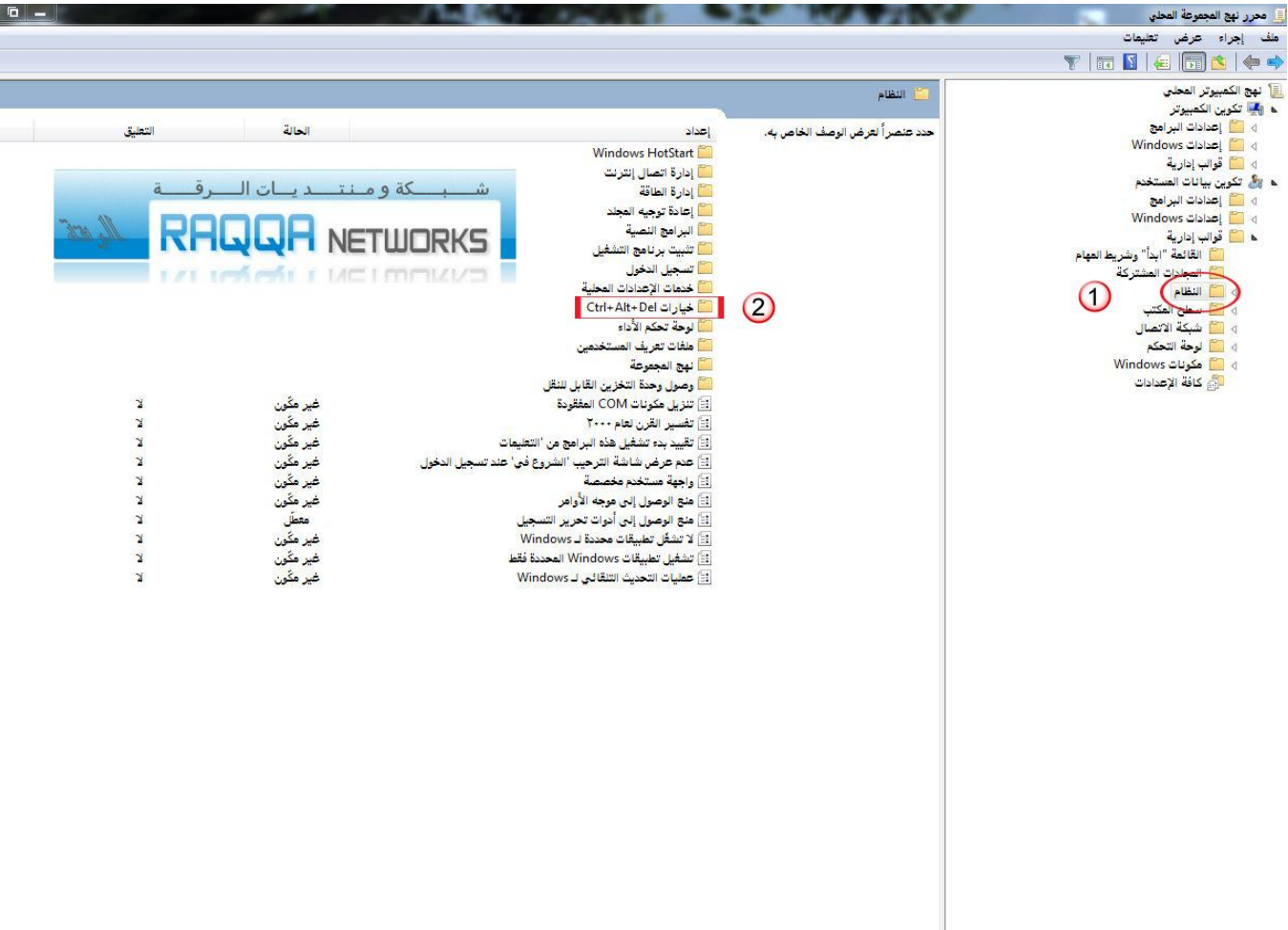
وننقر مرتين

وتظهر لنا الخيارات

فنختار

معطل أو غير مكون

شرح بالصور لطريقة تشغيل ادارة المهام :



ننقر مرتين على خيارات Ctrl+Alt+Del

فتظهر لنا

كالصورة :



محرك نيج المجهزة المحلي

Ctrl+Alt+Del خيارات

التعليق	الحالة
لا	غير مَكُون
لا	غير مَكُون
لا	غير مَكُون
لا	غير مَكُون

إعدادات إدارة المهام

إزالة إدارة المهام

تحرير إعدادات النيج

المتطلبات: Windows 2000 على الأقل

الوصف: منع المستخدمين من بدء تشغيل إدارة المهام (Taskmgr.exe).

نيج الكمبيوتر المحلي

إعدادات البرامج

Windows إعدادات

قوائم إدارية

تكوين بيانات المستخدم

إعدادات البرامج

Windows إعدادات

قوائم إدارية

القائمة "ابدأ" وضبط المهام

المجندات المشتركة

النظام

إزالة إدارة المهام

الإعدادات السابقة

الإعدادات التالية

تعليق: غير مَكُون

ممكن

معتل

مدعم في: Windows 2000 على الأقل

تعليمات:

منع المستخدمين من بدء تشغيل إدارة المهام (Taskmgr.exe).

إذا كان هذا الإعداد "معتكاً" وحاول المستخدم بدء تشغيل إدارة المهام، تظهر رسالة توضح أن هناك نيج يمنع تنفيذ الإجراء.

تتيح إدارة المهام للمستخدمين إمكانية تشغيل البرامج وإيقافها، ومراقبة الأداء أجهزة الكمبيوتر، وعرض كافة البرامج قيد التشغيل على أجهزة الكمبيوتر ومراقبتها بما في ذلك خدمات النظام، والبحث عن الأخطاء القابلة للتنفيذ الخاصة بالبرامج، وتغيير أفضلية العملية التي يتم تشغيل البرامج بها.

خيارات:

موافق

إلغاء الأمر

تطبيق

شبكة ومنتجات الرقعة

RAQQA NETWORKS

الفيروس يقوم بتعطيل إدارة المهام من نيج الكمبيوتر المحلي ونحن سنقوم بتنشغيلها

موسج قياسي

إعدادات/إعدادات

ازالة ادارة المهام نختار معطل

٢ - حل مشكلة أيقاف موجه الاوامر :

موجه الاوامر :

Run

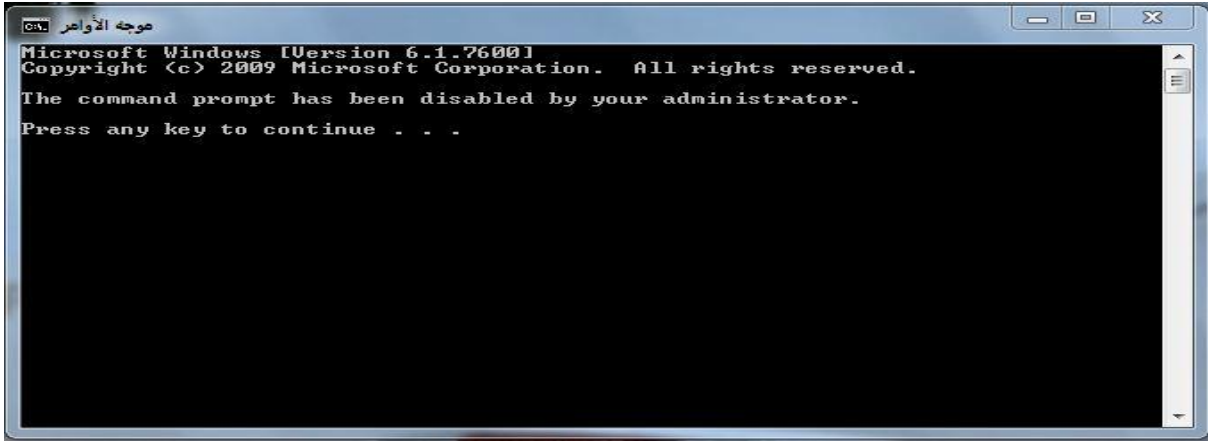
اداة مهمة للذين يتعاملون مع بيئة DOS الدوس

المشكلة كالتالي :

The command prompt has been disabled by your administrator.

موجه الاوامر تم تعطيله من قبل المدير "المسؤول".

لاحظ الصورة :



عمل الفيروس:

منع المستخدم من الوصول الى وجه الاوامر
(طبعا عن طريق محرر المجموعة المحلي)

حل المشكلة :

ندخل الى **محرر المجموعة المحلي** (ذكرنا طريقة الوصول اليها)

عن طريق الامر : gpedit.msc

+

تكوين بيانات المستخدم + قوالب ادارية + النظام + منع الوصول الى وجه الاوامر

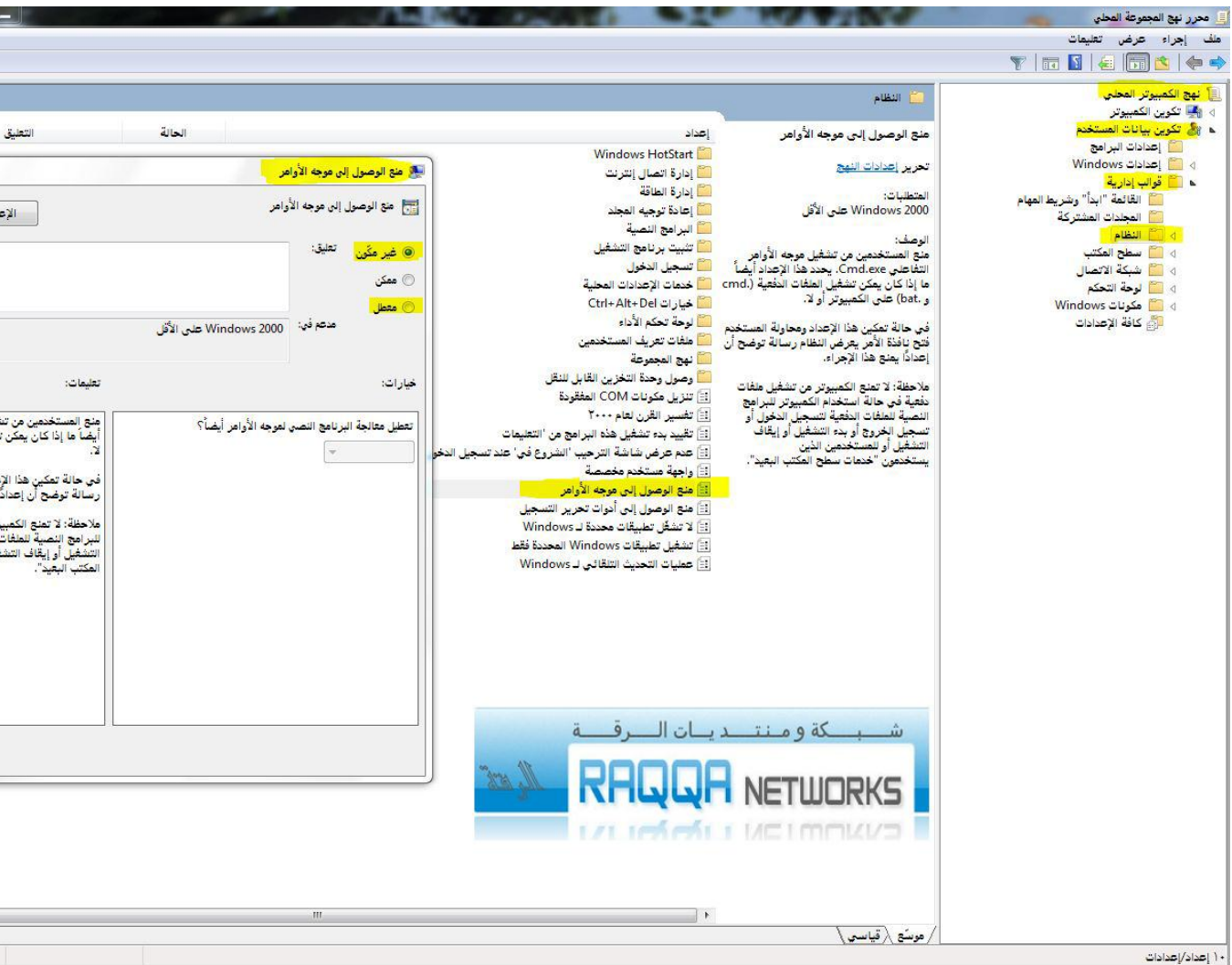
ونختار:

معطل أو غير مكون

موافق

شرح بالصور :

.....



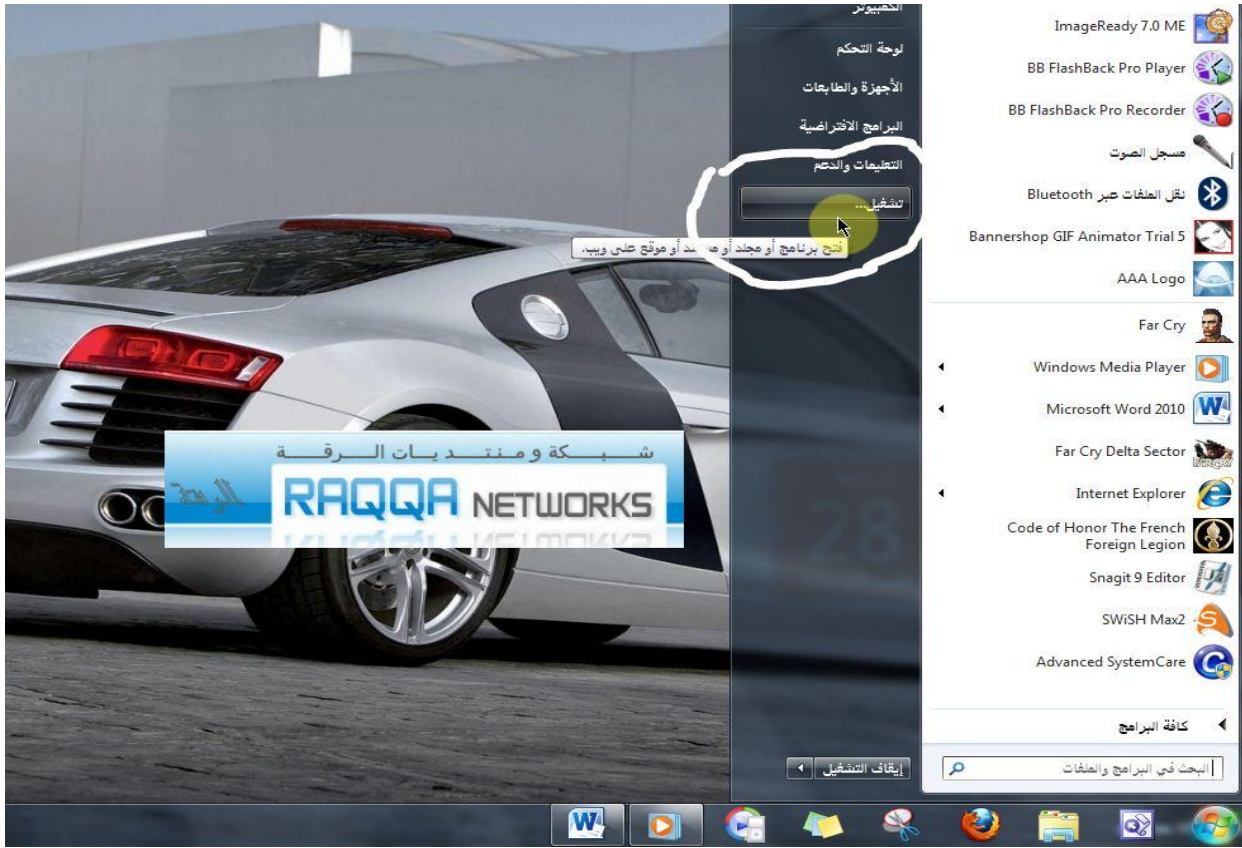
صورة توضح طريقة تشغيل / إيقاف محرر الاوامر

٤ - طريقة إضافة الامر تشغيل الى القائمة أبدأ على نظام win7

مربع الحوار تشغيل لا يوجد في القائمة أبدأ مباشرة في نظام win 7 يكون موجود في البرامج الملحقة

سنشرح طريقة إضافته

لاحظ الصورة :



صورة توضح مكان الامر تشغيل في القائمة أبدأ مباشرة على نظام win7

طريقة الاضافة :

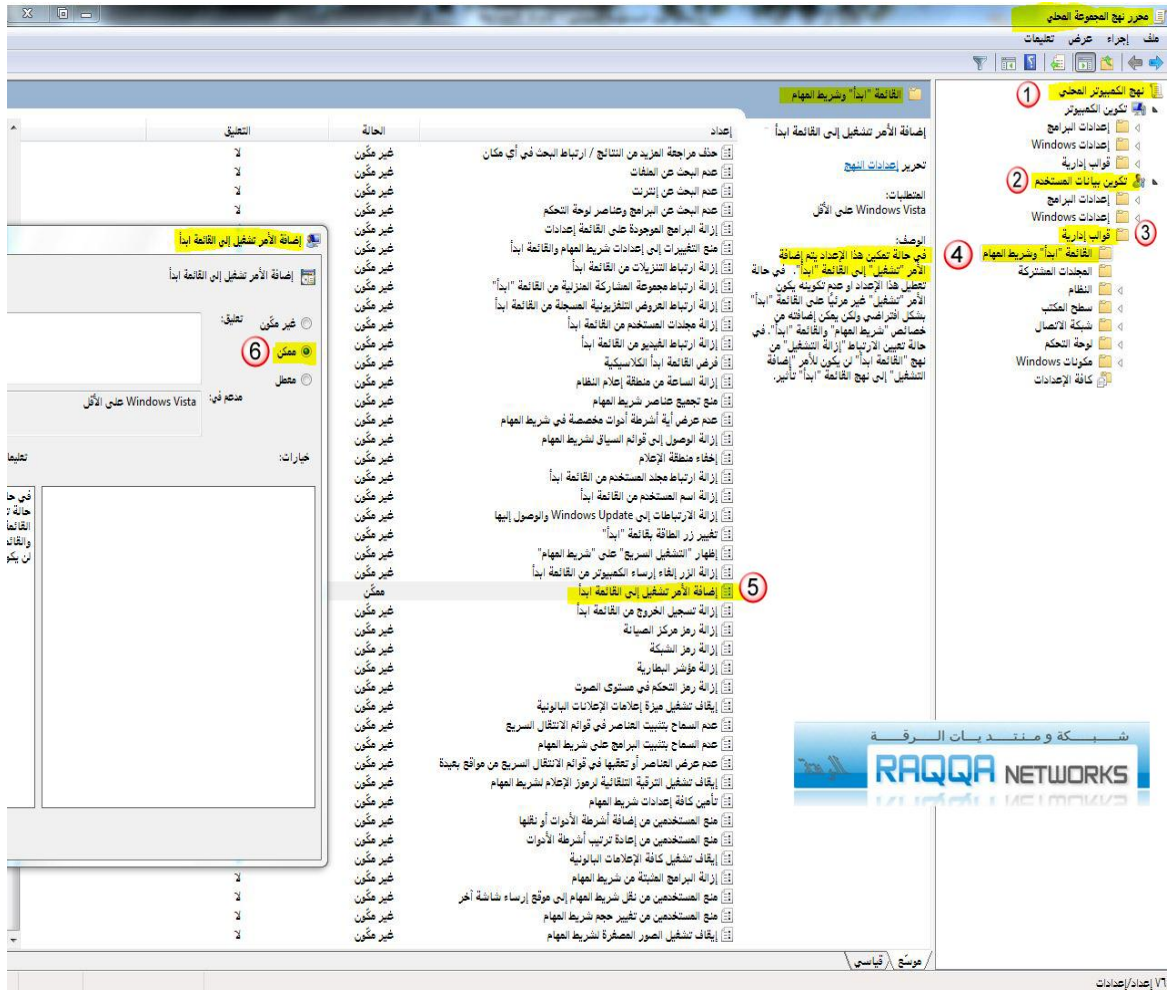
محرر نهج المجموعة المحلي + تكوين بيانات المستخدم + قوالب إدارية + القائمة أبدأ وشريط المهام + أضافة الامر تشغيل الى القائمة أبدأ

ننقر عليها ونختار ممكن

نم

موافق

كما في الصورة :



صورة توضح طريق ة إضافة الامر تشغيل الى القائمة ابدأ

الى هنا نصل الى نهاية الدرس

خاتمة :

من خلال محرر نهج المجموعة سنكتشف الكثير من الاعدادات الى التي تقوم بإيقافها الفيروسات

كما تستطيع تخصيص الكمبيوتر كما تشاء



كما نحاول تسهيل استعادة الإعدادات بشكل اسهل للمستخدم
عن طريق الاسطوانات التي تقوم بأوامر جاهزة تسهل استعادة الاعدادات
وهي تكون معاكسة تماما للفيروسات أي هندسة عكسية ولكن بشكل مبسط -_-
ولكن الوقت للأسف ضيق
وننتظر اكتشافاتكم ومناقشاتكم

للمشاركة نرجو منكم

زيارة المنتدى :

شبكة ومنتديات الرقة

<http://www.araqqa.syriaforums.net>

ووضع مناقشاتكم في قسم صيانة الكمبيوتر

ولأي استفسار راسلنا على البريد التالي :

raqqanetworks@gmail.com

جميع الحقوق محفوظة © ٢٠١١-٢٠١٢ لشبكة ومنتديات الرقة
