تقدم

الترتيبات الأمنية للحواسيب الجهادية

(الجزء الثاني)

الحمد لله وحده والصلاة والسلام على من لا نبي بعده,
تحدثنا في الجزء الأول من هذه السلسلة عن كيفية حماية الحاسوب باغلاق الثغرات المكشوفة للـ widows XP.
نبدأ الآن في الخوض في ما هو أعمق و اهم, وهو كيفية حماية الجهاز مما هو دخيل علينا.
في عالم النترنت هناك ثلاث أعداء خطرين:
التروجان و الفيروس و الهاكر, وسنستعرض كل هذا في فقرات مختلفة نعرف من خلالها بالخطرثم كيفية ردعه.

I التروجان و كيفة التخلص منه

I-1\ ما هو التروجان؟

التروجان هو برنامج تجسس و له أسماء أخرى مثل مخدم (Server) أو اللاصق (Patch) أو الجاسوس (Spy) لكن مبدعين هذا النوع من الملفات يفضلون الأسماء الرنانة و اسم تروجان هو نسبة إلى حصان طروادة. لكن مع اختلاف المسميات فهو برنامج تجسسي يجعل من حاسبك مخدم لحاسب الجاسوس, أي يتمكن الجاسوس (و هو الشخص الذي بعث إليك هذا التروجان) من التحكم بجهازك و كأنه أنت, لكن مع الأخذ بعين الاعتبار أن ذلك فقط في حال أنت متصل بالإنترنت أو الشبكة و ليس هذا فقط بل و عندما يعرف أنك على الإنترنت أما غير ذلك فهو لا حول له ولا قوة.

2- I\ كيف يلج التروجان إلى حاسب؟

1- عن طريق برامج المحادثة مثل Microsoft chat و ICQ و Mirc و MSN و Yahoo .. الخ.

فلا تستقبل أي ملف مهما يكن و خاصة التي يكون امتدادها exe و حالياً ظهرت برامج تقوم بتغير امتداد الصور إلى exe فبعض الهاكرز يستخدمها في الضحك على الضحايا و يقول لهم أنها صور مغير امتدادها إلى exeو لكنه قد يدس التروجان بداخلها أو قد تكون هي التروجان بحالها.

لذلك أنصح بعدم إضافة إلا من تعرفهم و إذا صادفت أي شخص لا تعرفه و شككت فيه فقم بعمل حظر ثم حذف, لكن إذا كان في جهازك تروجان و حظرته فسوف يدخل و أنت لا تعلم لأن الحظر لن يفيد ما دام الخادم في جهازك يستقبل أوامر العملاء.
وسنفسر, إن شاء الله وقدر, في الجزء الثالث من هذه السلسلة كيفية إنشاء تشات خاص بك وأصدقائك وتستغني بذلك عن كل هذه البرامج العميلة.

2- عن طريق البريد الالكتروني: لذا قم بحذف جميع الرسائل المجهولة و التي لا تعرف من هو مرسلها.

3- عن طريق تحميل برامج من مواقع مشبوهة.

4- عن طريق المنتديات التي تفعّل خاصية html قد يأتي من هو حاقد على المنتدى و يزرع الكود في رد لموضوع أو في موضوع جديد.

3- I\ كيف أتخلص من التروجان إذا أصاب جهازي؟

هناك طريقتين الأولى يدوية والثانية آلية, وسنبدأ باليدوية حتى نتأكد من خلوا أجهزتنا تماما من أخطر انواع التروخانات, ثم ننتقل إلى الطريقة الأتوماتكيةز

3-1- I\ الطريقة اليدوية:
قبل كل شيء يجب أن تعرف أن الملف التجسسي إذا أصاب جهازك فإنه سوف يستوطن في واحد على الأقل من الأماكن التالية:

1- في الريجستري .

2- في الملف Startup .

3- في الملف System.ini .

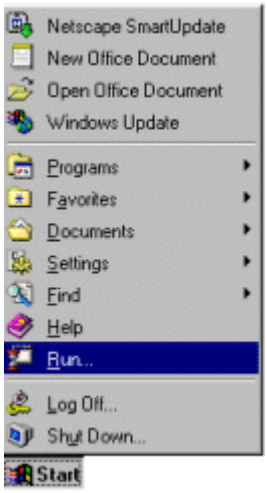
4- في الملف Win.ini .

أما للتخلص منه فإليك الطريقة..

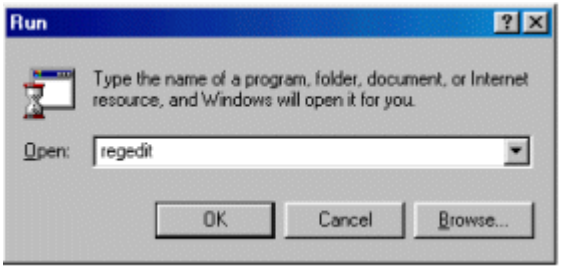
3-1-1- I\ الطريقة اليدوية في الريجستري:

بدخول دفتر التسجيل(Registry) و اتباع التالي:

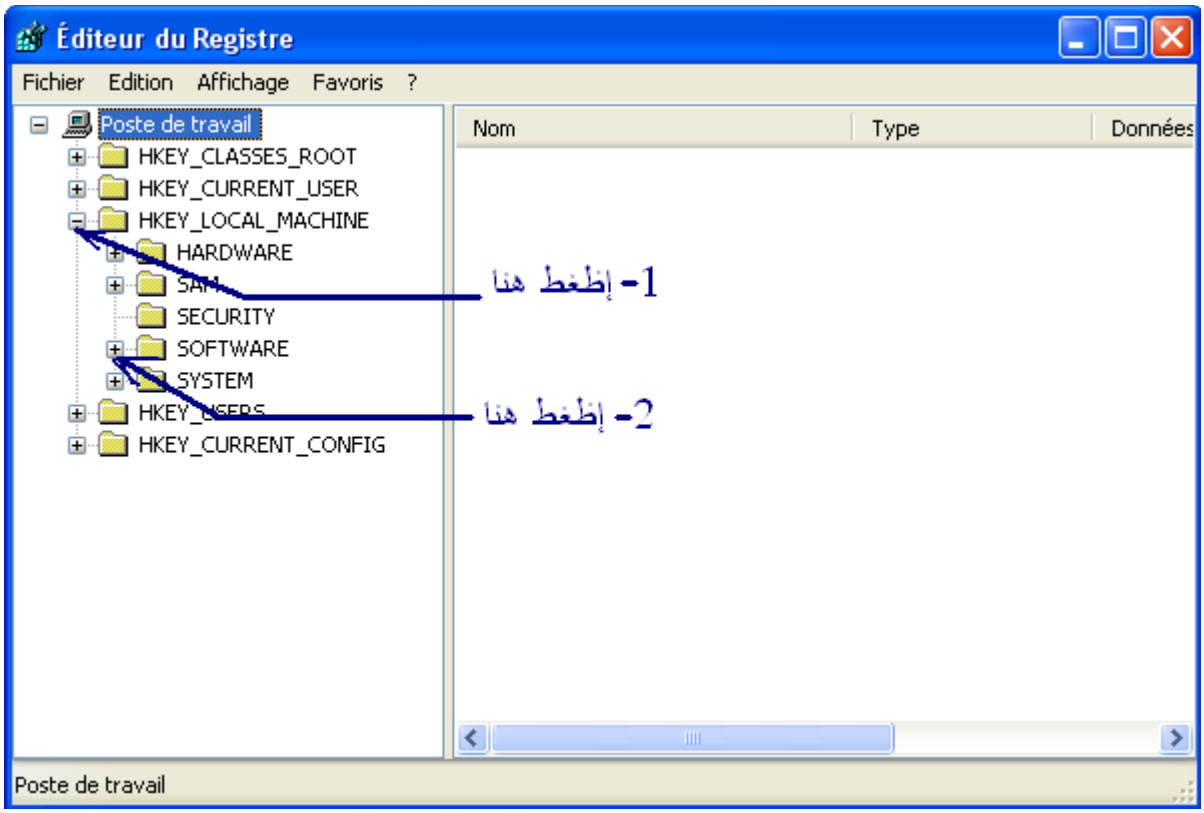
Start و الضغط على زر run



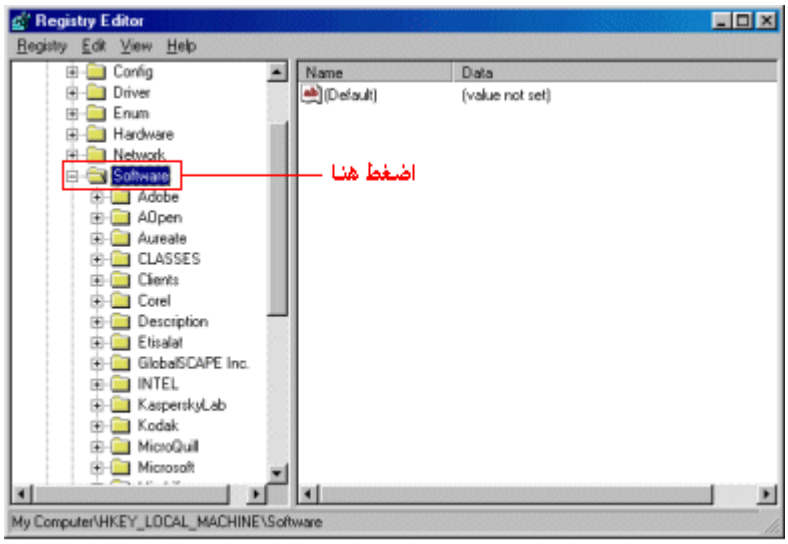
بكتابة (regedit) في المكان المخصص ستظهر نافذة دفتر التسجيل



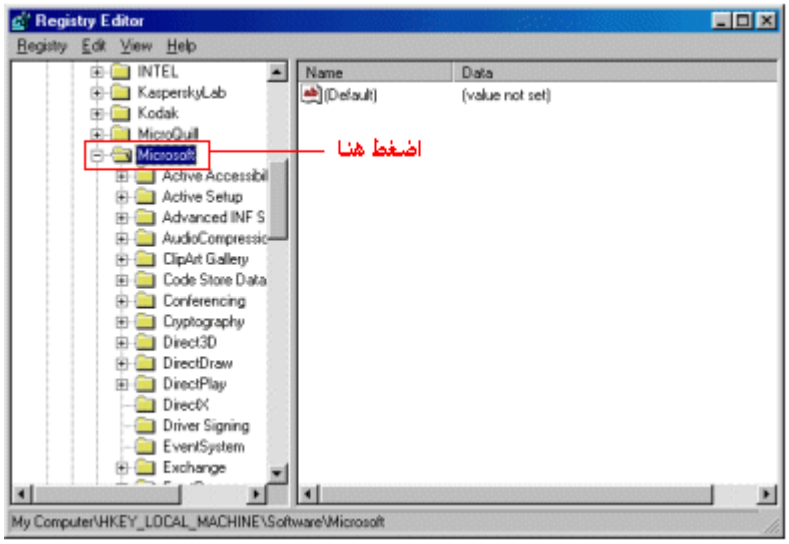
بالضغط على HKEY-LOCAL-MACHINE



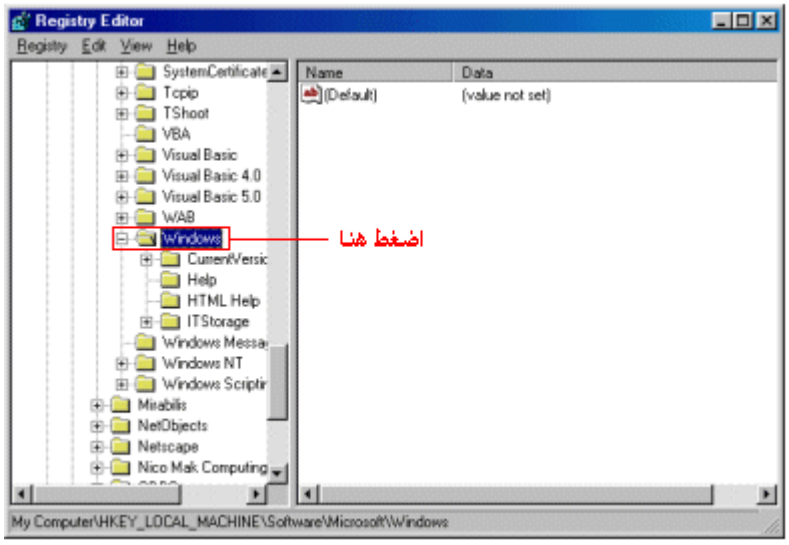
ستظهر قائمة أخرى, و باختيار Software



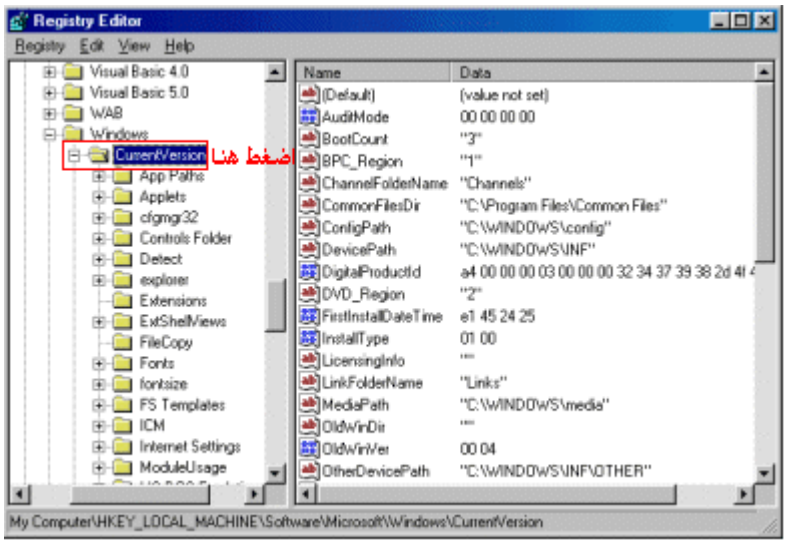
ثم الضغط على زر ال Microsoft ستظهر قائمة أخرى



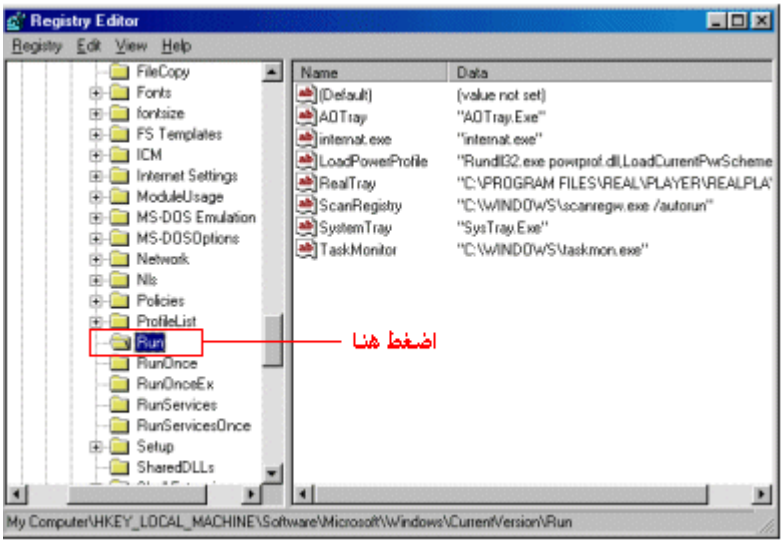
باختيار Windows



ستظهر قائمة أخرى أيضا, بعدها يتم الضغط على Current Version



و أخيراً بالضغط على Run

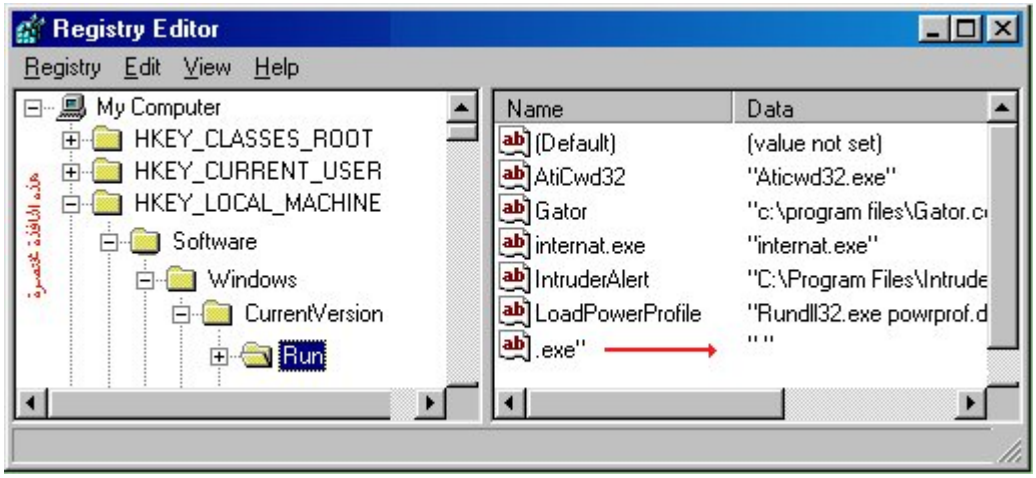


توجد قائمتان

الأولى (Name) و فيها اسم الملفات التي تعمل بقائمة بدء التشغيل للجهاز

الثانية (Data) و فيها معلومات عن الملف و امتداد ه أو البرنامج

من القائمة الثانية نستطيع معرفة ملف التجسس حيث أنه لن تكون له أي معلومات أو امتداد مثل الشكل التالي



فنقوم بحذف من دفتر التسجيل ما هو مريب و خطر:

- **الخطر الأول Back Oriface : اسم الملف Server وهو متغيير من مكان لآخر ولكن امتداده دائما Exe لكن يمكنك معرفته كون اسم الملف Server و تظهر بعده مسافةو من ثم .exe عندما تجد الملف الغه تماما ..**

- **الخطر الثاني Net Bus النسخة قبل 2000: هو الاكثر انتشارا على الشبكة .حجمه 470 كيلو بايت يستخدم المنافذ 12345 و المنافذ 12346و هو يمكن المخترق من السيطرة شبه الكاملة على جهازك,**

ابحث في القائمة على اليمين عن NBsvr.exe هذا هو اسم الملف في الغالب, عندما تجد الملف الغه تماما.

- **الخطر الثالث Heack'a Tack'a: يستخدم بروتوكل FTP مما يصعب الوصول اليه.يستخدم المنافذ رقم 31785 و 31787 و 31789 و 31791. ابحث عن Explorer32 و الذي يوافق المسار C:\WINDOWS\Expl32.exe و قم بحذفه**

- **الخطر الرابع NetSphere : يستخدم المنافذ TCP 30100 - TCP 30101-TCP 30102**

ابحث في الجهه اليمنى عن c:\windows\system\nssx.exe و قم بحذفه.

- **الخطر الخامس: إيجاد أي ملف بإسم من هذه الأسامي:**

  - **Explorer32**
  - **WINDOWSEXPL32.EXE**
  - **RunDLL32r**
  - **PATCH.EXE**
  - **EXPLO32**

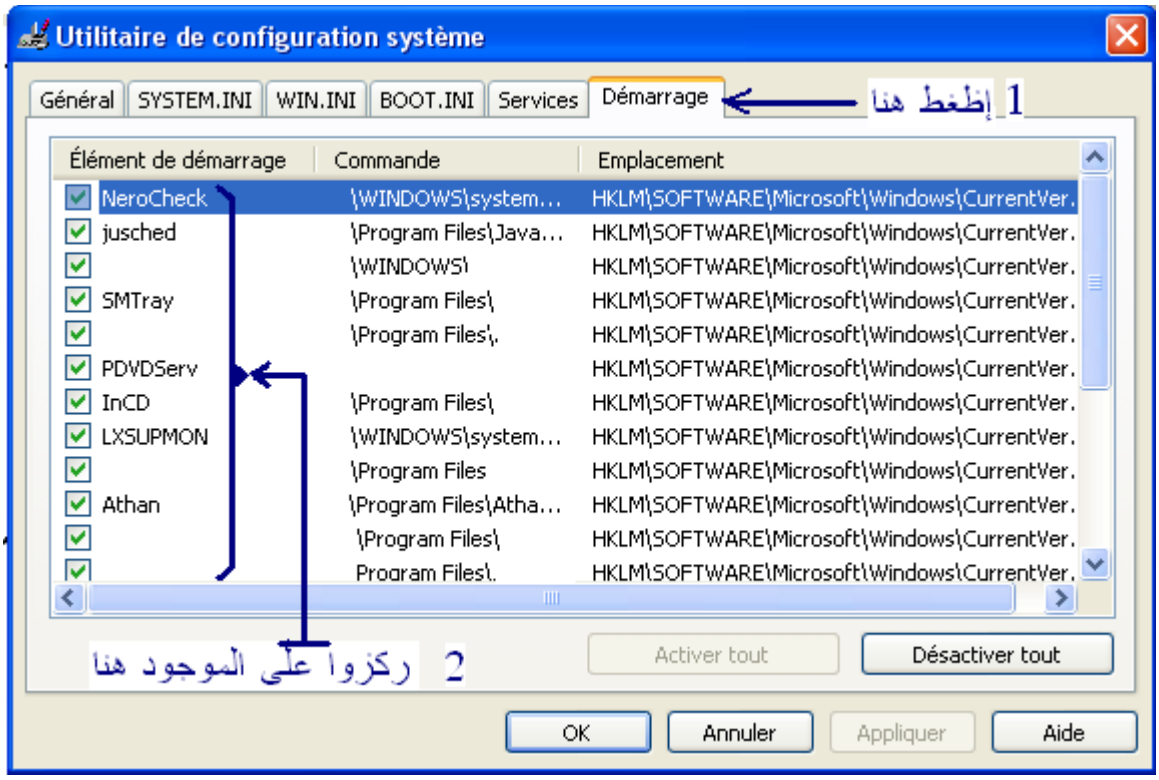
2-1-3- I\ الطريقة اليدوية في الملف Startup:

1-اضغط على زر start

2-اختر run

3-اكتب: msconfig

ثم اختر Start UP و من هناك ابحث عن اسم التروجان و غالباً ما يكون اسمه على الاسماء التي ذكرناها فوق, ثم إذا وجدته أزل علامة الصح من أمامه ثم اعد تشغيل الجهاز.



بصفة عامة إذا مررت بالمرحلة الأولى بسلام و إن شاء اله سوف لن تجد شيئا هنا, وعلى كل إذا أردت ان تعرف ما هي هذه البرامج التي تراها, فما هي إلا البرامج التي تنطلق إبان فتحك للحاسوب, ويمكنك كتابة كل منها على حدة في google.com ثم اقرأ ما تجده مفسرا هناك في المواقع المختلفة.

3-1-3- I\ الطريقة اليدوية في الملف system.ini:

-نختار الأمر تشغيل (Run) ثم نكتب هذا الأمر (system.ini) ثم نضغط مفتاح الإدخال .
- ستظهر لنا شاشة .. نلاحظ جيدا محتويات هذه الشاشة :
أولا نبحث عن سطر فيه هذا "System.ini ===>Shell=Explorer.exe rundll16.exe
فإن كان كذلك نحذفه وإلا فالحمد لله, من قبل ومن بعد.

ثانيا ,في الويندوز 2000 و الويندوز XP .. نلاحظ السطور الأربعة الأخيرة

EGA80WOA.FON=EGA80850.FON
EGA40WOA.FON=EGA40850.FON
CGA80WOA.FON=CGA80850.FON
CGA40WOA.FON=CGA40850.FON

دقق النظر اذا كانت القيم مثل الاربع اسطر الي فوق
فهذا يعني ان جهازك نظيف والحمد لله, من قبل ومن بعد.

اما اذا كانت القيم مثل الاربع اسطر الي في الاسفل معنى هذا ان جهازك به ملفات تجسس

EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

4-1-3- I\ الطريقة اليدوية في الملف win.ini:

-نختار الأمر تشغيل (Run) ثم نكتب هذا الأمر (system.ini) ثم نضغط مفتاح الإدخال .
- ستظهر لنا شاشة .. نلاحظ جيدا محتويات هذه الشاشة :

نبحث عن سطر فيه هذا:

Run=????.exe
أو
Load=????.exe

ونقاط الإستفهام تدل عن أي شيئ , أي إسم كان.. فالموجود هو إسم برنامج لهاكر متصل على الجهاز.
فأن وجد سطر بهذه المواصفات نحذفه على الفور , ولا ننسى التسجيل قبل غلق الملف.

الخلاصة:
كا ما قمنا به إلى حد الأن هو التأكد يدويا من سلامة الجهاز, أرجوا ان لا تكونوا قد تعرضتم إلى أي نوع من التروخانات إلى حد الآن, أقصد التروجانات الخطيرة, وعلى كل أفضل ثلاث مواقع يقدم لك الاستفسار الكامل عن أي تروجان هم

/http://www.dark-e.com/archive/trojans

http://www.moosoft.com/tdbindex.php

أما الآن فسنمر إلى الطريقة الآلية لتنظيف الجهاز

4-2-3- I\ الطريقة الآلية:

هنا الأمر سهل, فما عليكم إلا انزال أحد البرامج التالية وتشغيلها على حاسوبك ولقد إخترت إليكم أقوى برامج, بإعتراف المتخصصين في الميدان.

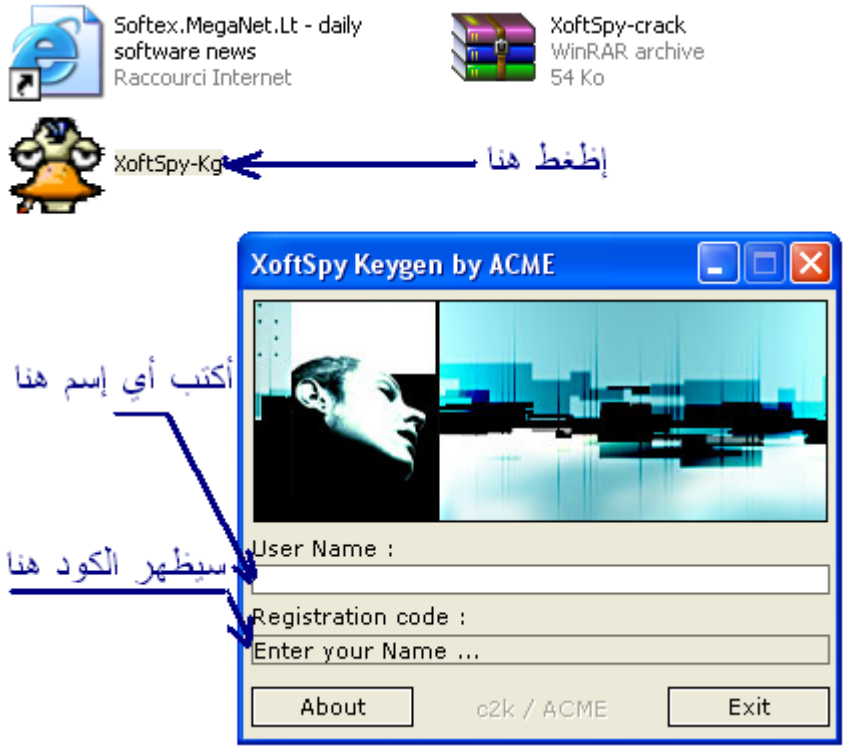
Xsoftspy

رابط التنزيل : http://paretologic.com/XoftSpy421_138.exe

الكراك: http://sendmefile.com/00221589

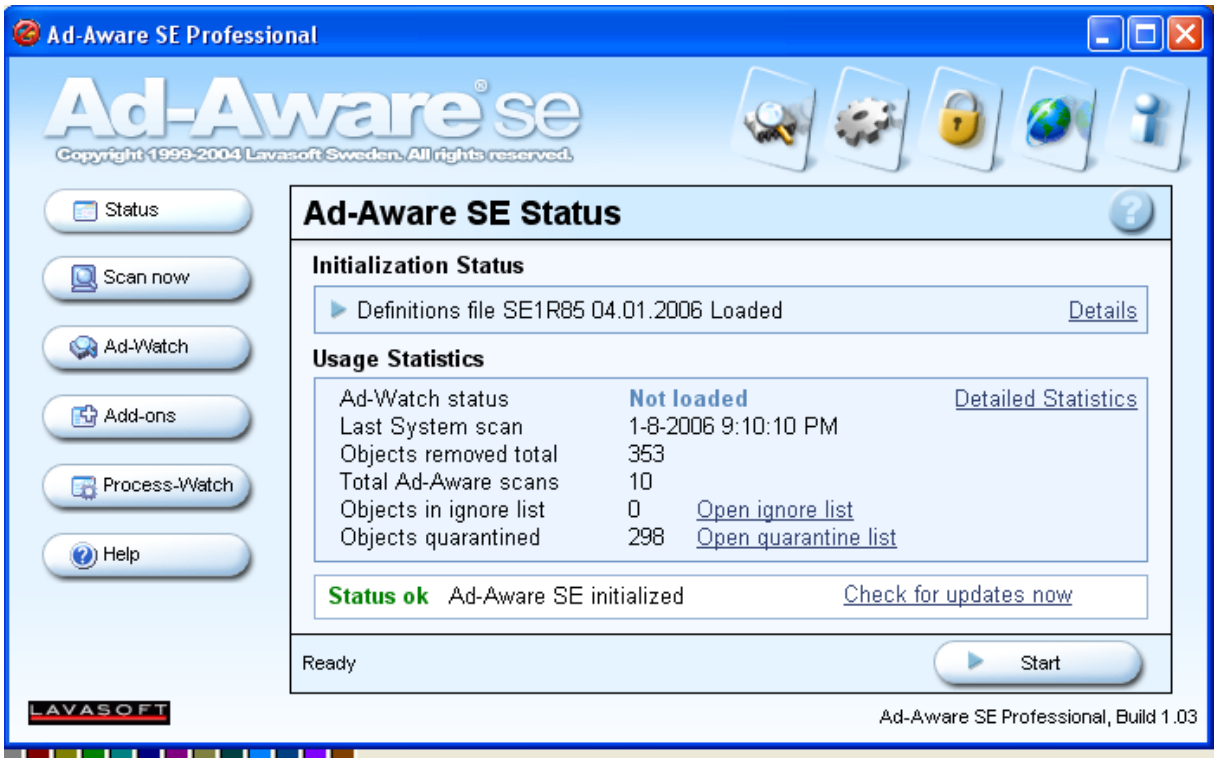
وتشغيل الكراك كالتالي:


Softex.MegaNet.Lt - daily
software news
Raccourci Internet
XoftSpy-crack
WinRAR archive
54 Ko
XoftSpy-Kg
إظغط هنا مرتين


Softex.MegaNet.Lt - daily
software news
Raccourci Internet
XoftSpy-crack
WinRAR archive
54 Ko
XoftSpy-Kg
إظغط هنا
أكتب أي إسم هنا
سيظهر الكود هنا
XoftSpy Keygen by ACME
User Name :
Registration code :
Enter your Name ...
About
c2k / ACME
Exit

Ad aware

http://download.lavasoft.de.edgesuite.net/public/defs.zip



Spybot

http://www.tucows.com/preview/310138

بالنسبة لهذا البرنامج النسخة المجانية كافية .

إنتهى موضوع التروخان وهو الأعمق والأصعب. وننتقل الآن إلى موضوع الفيروس والهاكر.

II الفيروس والهاكر:

قمت بجمع الهاكر والفيروس في قسم واحد نظرا لخاصيتهم المشتركة في إقتحام الحاسوب بدون علمنا. أبدأ أولا بتعريف الهاكر:

هم مبرمجين للحاسب الالي وقادرين على حل اي اعطال تتعلق بالحاسب ولديهم علم بلغات البرمجه. ولكن ليس شرط ان كل المبرمجين هم هكرز. والهكرز احياناً يكونون مجموعه واحده واحياناً لا. ولكن لو أردنا تعريف الهكر تحديداً:
هو عباره عن مخرب أحياناً يكون لديه هدف واحياناً ليس لديه هدف لكن هدفه الاساسي هو الاختراق والعبث في خصوصيات الاخرين دون علمهم ولايفكر بالاضرار التي نتجت عن إختراقه.
تــعريــف الإخـــتـــراق:
هو القدره على الوصول لهدف معين طبعاً بطريقه غير مشروعه سواء أجهزه شخصيه أو أجهزه حكوميه وذلك بسبب ثغرات أمنيه موجده في نظام الحمايه لدى أجهزة المستخدمين. ولدى إقتحامهم يركبون برنامجا لاصقا يتحكمون به عن بعد في جهازك.
مثال حي: من خلال تتبعي لألد أعدائنا في الانترنت وهم فريق الهاغانا للإنترنت, صدمت بأن احدهم قد تمكن من الدخول على حاسوب احد الأعظاء المهمين في الجبهة الإعلامية و أخذ نسخة مصورة من شاشته, كدليل يريد ان يقدمه لسلطات ذلك البلد للقبض عليه (نلاحظ هنا اهمية تامين الجهاو من الإختراق) فقمت غيرة على أخي بالبحث عن هذا الوغد فلم أستطع الحصول عليه , ولكن ربـي رزقني غنيمة أسمن منه, إذ أنني تحصلت على زعيمهم وعلى أخص خصوصياته ونشرتها في الإنترنت, كل ما له علاقة بتميلاته من الدولة العبرية, الجماعات التي تتعاطف معهم, طبعا كل هذا وانا أعني ان السيد مقيم بأمريكا وهذه الدولة لا تسمح بأن يقام نشاط تجسسي على ترابها بدون علمها (سنفسر هذه النقطة في سلسلة جديدة عن الجغرافيا السياسية ,إن شاء الله وقدر) المهم هنا أحببتي ذكرت لكم أهمية الإختراق.

ولله الحمد قمنا في ما سبق بإلاغلاق أهم المنافذ للــحـاسوب. كما قمنا أيظا بفحص أهم الملفات التي قد يستعملها مخترق للوصول إلى حواسيبكم.
نبدأ الآن بتثبيت انظمة حامية من خطر الإختراق من قبل الهاكر أو الفيروس واخترت لكم برنامجين على التحديد نظرا لفعاليتهم وذلك باعتراف المخترقين أنفسهم: الـ ZONE ALARM و KASPERSKY ودعكم من الذي يقلك النورتن و..و.وو فالنورتن مثلا يبطأ حلسوبك إلى درجة توصلك في بعظ الأحيان لغلقه! والبرامج الأخرى لا تجد حل لبعض التروخانات إلا متأخرة !
المهم, أقدم لكم روابط تنزيل البرامج :

KASPERCKY

Kaspercky internet security
http://www.softpedia.com/progDownload/Kaspersky-Internet-Security---Beta-Download-20619.html
أو
http://download.softpedia.com/software/antivirus/kis6.en.msi

kaspercky Anti-virus

http://fileforum.betanews.com/download/Kaspersky_AntiVirus_Personal/1008918303/2

الرقم السري :
KAV 2006 - 2 desktop
187272B5-62F6-4CFF-BE82-D1B1FFD0A32E7

KAV2006
B2B66782-6AC0-4533-88F4-060BB929C9318

Zone alarm

http://www.zonelabs.com/store/content/company/products/trial_zaFamily/trial_zaFamily.jsp?dc=12bms&ctry=US&lang=en&lid=zassskulist2_trial

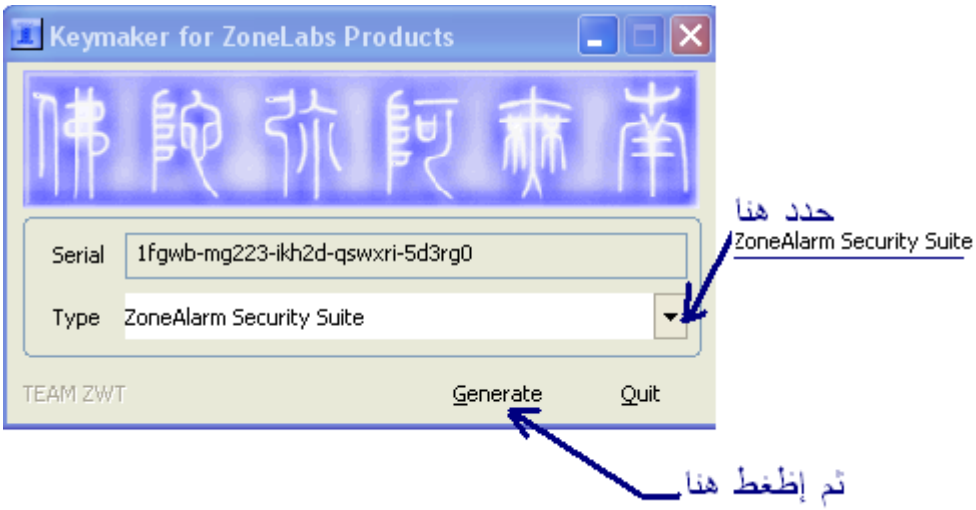
---

ثم

	ZoneAlarm® Internet Security Suite	ZoneAlarm® Pro	ZoneAlarm® Anti-Spyware	ZoneAlarm® Antivirus
	15 Day Free Trial	15 Day Free Trial	15 Day Free Trial	15 Day Free Trial
Features:	DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD
Basic Firewall	X	X	X	X
Triple Defense Firewall™	X	X	X	X
Anti-Spyware	X	X	X	
Antivirus Protection	X	إظغط هنا		X
Identity Theft & Privacy Protection	X	X		
Anti-Phishing & Spam Blocker	X			
Email Security	X	X	X	X
IM Security/Parental Controls	X			
Wireless PC Protection	X	X	X	X

ثم نزلوا الكراك من هنا
http://sendmefile.com/00222121
او من هنا
http://www.sendspace.com/file/q9q717

وطريقة عمله هي كالآتي



الآن نستطيع أن نظمن سلامة الجهاز, وللتأكد زوروا هذا الرابط وسيفحص لكم الثغرات على جهازكم وسيوافيكم باخبار سارة إن شاء الله..

- http://probe.hackerwatch.org/probe/probe.asp

ختاماً, نقوم بتقديم بعض النصائح للمحافظة على سلامة بريدك الإلكتروني من الإختراق.

أقدم لكم 27 نقطة في غاية الاهمية لحماية بريدك الإلكترني من السرقة:

1- -يجب ان تكون كلمة المرور طويلة جدا - وليس 5 او 7 خانات فقط والافضل ان تجعلها بما يقارب 20

خانة وذلك في الياهوو اما الهوتميل للاسف فلا يدعم اكثر من 16 خانة

2- يجب ان تحتوى كلمة المرور على خليط من الرموز والارقام والحروف تكون صغيرة وكبيرة :مثال %SFDH~297fj=-ZP

3 - يجب ان لا تكون كلمة المرور بسيطة بمعنى انك لا تتبع الطريقة الابجدية على الكيبورد بطريقة تسلسلية – يجب ان تكون بطريقة عشوائية مثال QWERTYUI&123ASD

4 - لا يجب ان تكون كلمة المرور عبارة عن ارقام تسلسلية او ارقام عشوائية فقط لان انت ممكن تشوفها صعبة لكن مع وجود البرامج المختصة تبقى عملية اكتشافها سهلة جدا مثال : 123456789

5 - يجب ان تكون كلمة المرور مختلفة عن اى معلومة حقيقية مختصة بك :رقم الموبايل او البلد او المدينة

6 - يجب ان تكون كلمة المرور بعيدة تماما على الكلمات المشهورة سواء اماكن او اشخاص ,لانها اول حاجة ممكن تخطر على بال اى احد و كذلك هناك

برامج مختصة ب هذا الموضوع.

7 - يجب ان يكون عندك ثقة بالشخص المحاور لك ,لان ممكن بعد فترة يبدأ يكشف ويجمع معلومات عنك ممكن تفيده فى اختراق بريدك الإلكترني .

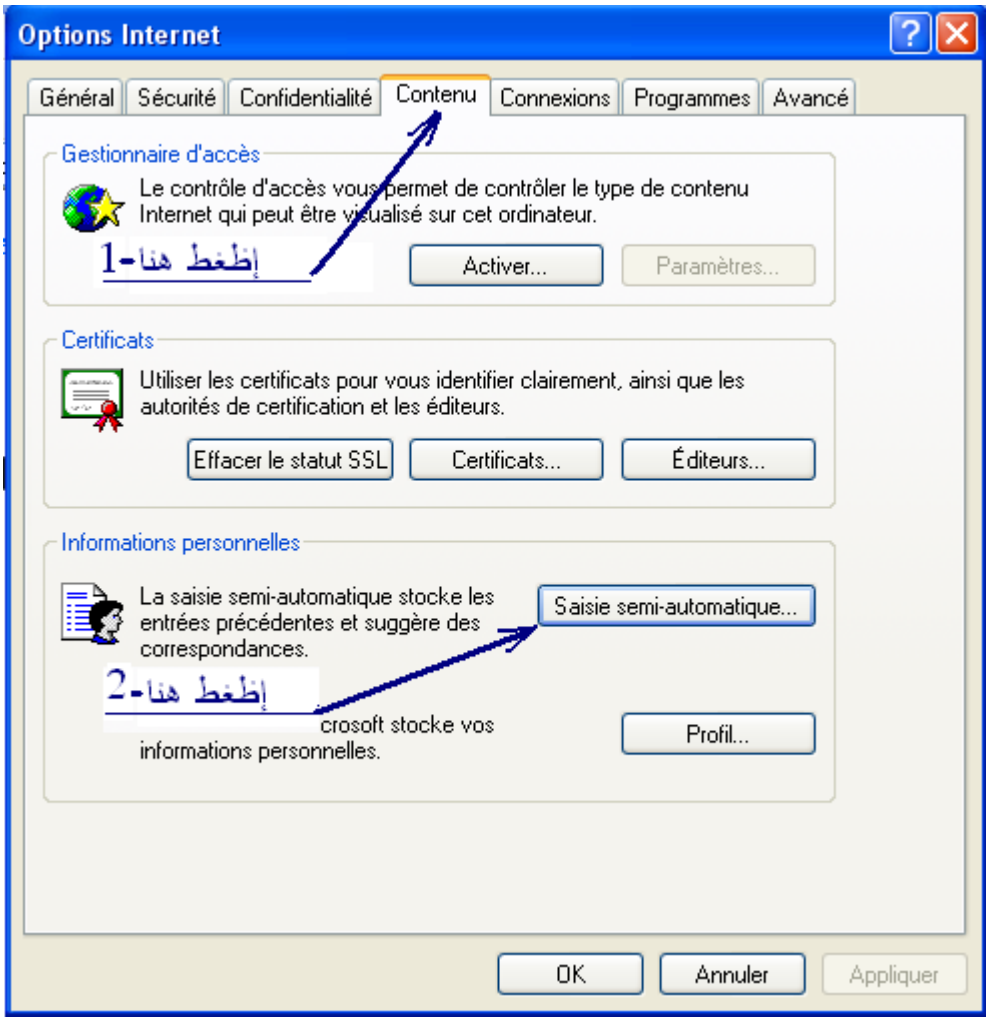
8- لازم تغيير كلمة المرور بين الحين والآخر, لنقل دوريا كل شهر مثلا.

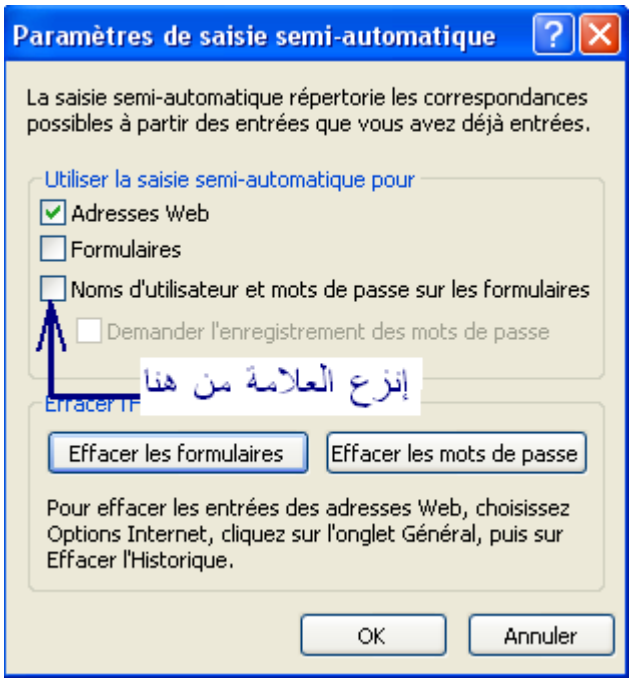
9- ضع بريد إلكترني جديد للمنتديات ,وتخليه للاختبار وتبتعد عن بريدك الإلكترني الاساسى , و لا تستقبل فيه معلومات مهمة.

10- حين استخدام المسنجر لازم يكون عندك ثقة فى الشخص المحاور لك , لانك لو تكلمت معاه بالصوت ممكن يحدد رقم الاى بى عن طريق برنامج كراكرز ثم يتحصل على عنوانك الشخصي.

11- دع ايميلك الاساسى على مواقع غير مشهورة لان اغلب البرامج والهاكر مسخرين طاقاتهم للمواقع المشهورة رغم مستوى الامن العالى اللي فيها) الياهو والهوتميل(... جرب مزودات خدمة جديدة مثل مكتوب وجووجل... الخ

12- الحذر الحذر من موضوع خاصية الاكمال التلقائى فى كلمات المرور , بمعنى انك لما تجى تكتب اول حرف من ايميلك يظهر لك , هذا معناه انه متخزن فى الجهاز هو او الباسورد و هذا خطر جدا وحتى تتفادى الموضوع ده فى الاكسبلور روح على الادوات - خيارت الانترنت محتوى الاكمال التلقائى وشيل كل علمات الصح اللي فيه كلها واوعى تستخدم الخاصية دي فى المسنجر او الياهو بوضع علامة صح فى البرنامج جنب عبارة : تذكر بياناتي.





13- ان فقدت كلمة السر لبريدك الإلكترونى ولا تحاول ان ترجعه ليه لان البرامج المستخدمة فى الاستعادة يا اغلبها فيها تروجانات وممكن تقع فى فخها, وابتعد عن المواقع اللتي تدعى امكانية اعادتها

14- لما تنتهى من تصفح البريدك الإلكترني,لا تنسى SIGN OUT وخصوصا فى مقاهى الانترنت.

15- عدم ارسال روابط مواضيعك عن طريق المسنجر حتى تحافظ على خصوصيتك فى المنتديات

16- تجنب فتح المرفقات المجهولة اياً كانت مغرية لانها ممكن يكون فيها تروجانات مخصصة للبريد.

17- اختر بحرص المنتدى الذي ستشارك فيه. لان أغلب الناس تجعل كلمة المرور الاساسية فى البريد الخاص نفسها كلمة المرور فى المنتديات .

18- فى حالة استيلاء اى حد على ايميلك عليك باتباع الخطة التالية وهى تدمير البريدك الإلكترنيالخاص بك عن طريق برامج كتير موجودة بتقوم بارسال الاف الرسائل وبكده حتصعب عليه مهمة ملاحظة الرسائل المهمة اللي فى بريدك نتيجة الكم الهائل من الرسايل وتخلى عناوين الموضوع متشابهة تماما مع المواضيع المهمة .

19- فى حالة اردت استعادة بريدك وتمتلك كلمة المرور والبيانات الخاصة به تاكد من المسؤول عن البريد - يعنى من الصفحة الرئيسية الخاصة بالمساعدة.

20- دايما اعمل عملية مسح نهائى لمحتويات البريد ولو كان فى شىء مهم احفظها فى مكان امن : فلوبى سى دى او تشفيرها - والسبب انه فى حالة الاستيلاء عليه يكون البريد لا قيمة له وبالتالى سوف يعيده ولا يهتم به ان شاء الله

21- تأكد من تحديد عنوان بريد إلكترني بديل او ثانوي لبريدك و اجابة السؤال السري حتى لو نسيت كلمة السر او حبيت ترجعها او تغيرها يبعتهالك على بريدك الإلكترني البديل.

-

22- يغفل البعض عن ماتحتويه المنتديات من أساليب تساعد لكشف الرقم السري, يقوم شخص ويشترك بمنتدى وعندما يطلب منه الاسم والرقم السري يقوم بوضع الرقم السري مطابق لما هو موجود في الإيميل, لكنه يغفل أن المراقب العام يستطيع معرفة بيانات كل مستخدم وحتى رقمه السري وبهذا يستطيع كشف بريده.

-

- **23- يغفل البعض عند دخوله لأحد المواقع ويكون لها وصله سريعه يضع فيها اسمه والرقم السري تنقله إلا بريده في الهوتميل أو الياهوو أو ماشابه, هل تيقن أن الوصله تنقله إلى ذلك الموضع؟؟؟.**
ألا يمكن أن تكون الوصلة كذبة, يعني تنقل بياناتك (الرقم السري والباسوورد), نحو بريد الإلكترني صاحب الموقع وبالتالي عرف اسمك والرقم السري!!.

-

- **24- يقوم البعض عند دخوله للشات وخاصة مايكروسوفت بأن أحد قد بعث له ملف وغالبا مايكون صورة فينخدع بأنها فيروس يقوم بتحطيم جهازه, ويعرف ذلك الفيروس بطريقة هي عندما يرسل لك الملف يظهر اسمه وامتداده ,إذا كان غير GIF أو JPG فهو فيروس يسأل البعض لما**

هذان الإمتدادين فقط, لأنهما الغالبان المستخدمان في عرض الصور , قد يرسل لك غير هذا الإمتداد مثل ZIP وهذا ذو حدين أنت لاتعرف مايتواجد به, أو PPS الذي هو عرض للباور بوينت فهذا لا شيء فيه ,ولكن الأفضل أن لاتستقبل أي ملف مالم تعرف مصدره الموثوق, وكل هذا انصحك بالإبتعاد عن هذا الشات وال ICQ لأنهم يكثر بهم المنافذ ومما يجعل محاولات إختراق جهازك كثيره ,لأنه يعرض بهما رقم الأي بي الخاص بك

25- يموت البعض إذا صمم له أحد توقيع بالفلاش, وهو لايعلم أنه قد يكون ملغوم, هل تعلم أنه بتوقيع فلاش واحد....قد يكون مستهدف من شخص واحد, يقوم بشل حركة جميع المنتديات, ولا يستطيع أحد الدخول للمنتدى إلا مصمم هذا التوقيع

إنتهى الجزء الثاني.

لا تنسونا من صالح دعائكم