الأكاديمية العربية الدولية
Arab International Academy

اسم المادة: كشف الاختراق والاستجابة

المحاضِر: م. خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

مقدمة

ما هي عملية الهاكينج أو التجسس؟

تسمى الاختراق بالإنجليزية (Hacking) .... و تسمى باللغة العربية عملية التجسس أو الاختراق....

حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في جهازك بطريقة غير شرعية ولأغراض غيرسوية مثل التجسس أو السرقة أو التخريب حيث يتاح للشخص المتجسس (الهاكر) أن ينقل أو يمسح أو يضيف ملفات أوبرامج

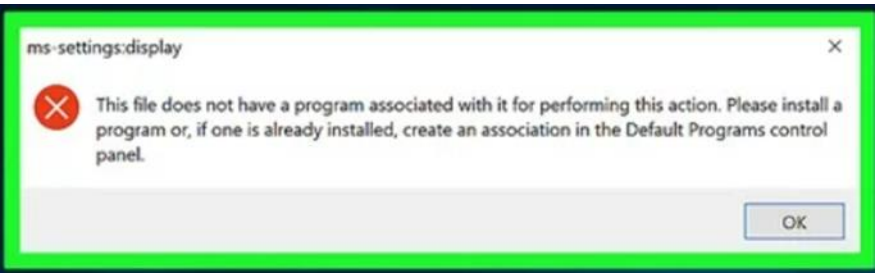
كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين..

من هم الهاكرز ؟

هم الأشخاص الذين يخترقون الأجهزة فيستطيعون مشاهدة ما بها من ملفات أو سرقتها أو تدمير الجهاز أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت..

العلامات الدالة على اختراق إلكتروني

1- لاحظ أي شيء غير طبيعي يحدث على شاشة الكمبيوتر. في الأغلب أنت تستخدم الكمبيوتر يوميًا، وبالتالي من الطبيعي أن تعرفه وتعرف طريقة عمله أكثر من أي شخص آخر. إذا كنت تعمل على الجهاز بشكل طبيعي لكن فجأة أصبح نظام التشغيل يقوم بأفعال غريبة، فالأسباب وراء ذلك قد ترجع إلى قدم مكونات الكمبيوتر أو وجود تلف من نوع أو آخر، لكن العلامات التالية تحديدًا قد تشير كذلك إلى تعرض الجهاز إلى الاختراق:



- اختفاء بعض الملفات على الرغم من أنك لم تحذفها، إذ تجدها محذوفة تمامًا أو تم نقلها إلى سلة المهملات.
- يوجد لديك برامج أو ملفات أساسية لا تعمل بشكل طبيعي أو ترفض أن يتم فتحها من الأساس.
- لا تقدر على تشغيل البرامج باستخدام كلمة السر المعتادة. ربما تجد أن كلمات السر الخاصة بك تم تغييرها.
- يوجد برنامج أو أكثر تم تثبيته على الكمبيوتر دون أن تكون أنت الطرف الذي قام بهذا الأمر.
- يوصل الكمبيوتر نفسه بشبكة الإنترنت بشكل متكرر في أوقات عدم استخدامك له.
- تم تغيير محتوى بعض الملفات دون أن تكون أنت الطرف الذي قام بهذه التغييرات.
- تصدر الطابعة خطوات غريبة. ربما ترفض طباعة ما توجهه لها من أوامر طباعة أو أن تطبع صفحات مختلفة عما حددته لها.

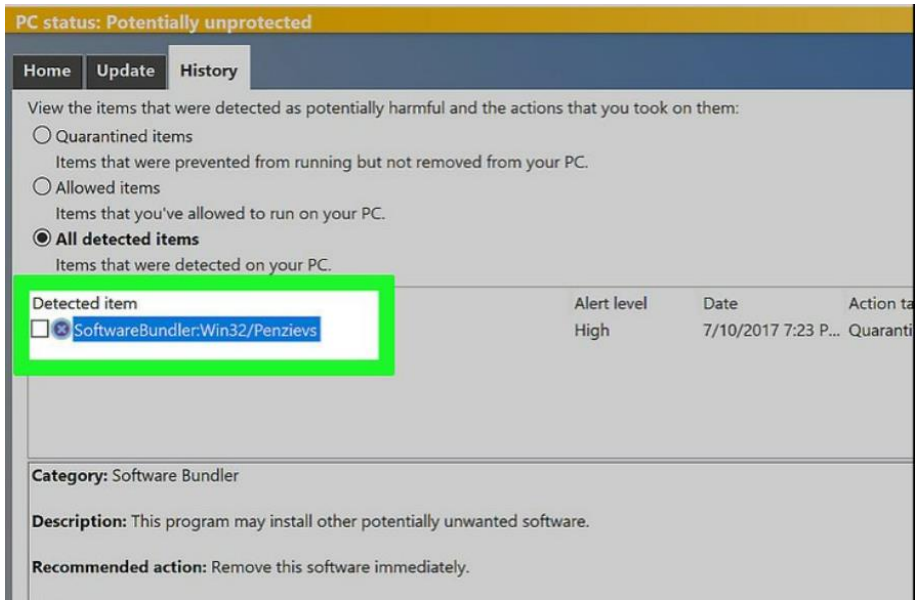
العلامات الدالة على اختراق إلكتروني

2- اتصل بالإنترنت. يمكنك من خلال هذه الخطوة أن ترى الكثير من العلامات الدالة على تعرضك للاختراق.

يرفض موقع أو أكثر أن يتم عملية تسجيل دخولك إليه بسبب تغيير كلمة السر. جرب مجموعة من المواقع التي تزورها بشكل معتاد؛ إذا لم تنجح كلمة السر الخاصة بك، فقد يرجع السبب وراء ذلك إلى تعرضك للاختراق. هل قمت بالتفاعل مع أي من رسائل البريد الإلكترونية المؤذية عن طريق الخطأ (أو رسالة بريد إلكتروني محتالة تطلب منك تحديث كلمة السر أو تغيير خيارات الأمان)؟

- يتم إعادة توجيه نتائج البحث الخاصة بك.
- تظهر نوافذ إضافية من متصفح الإنترنت. يمكن أن يتم تشغيل وإغلاق هذه النوافذ دون أن تفعل أي شيء؛ ربما تكون هذه النوافذ ذات لون أكثر قتامة إلا أنك سوف تكون قادرًا على رؤيتهم.
- إذا قمت بشراء اسم نطاق إلكتروني، فربما أنك غير قادر على الوصول إليه بمجرد إتمامك لعملية الشراء.

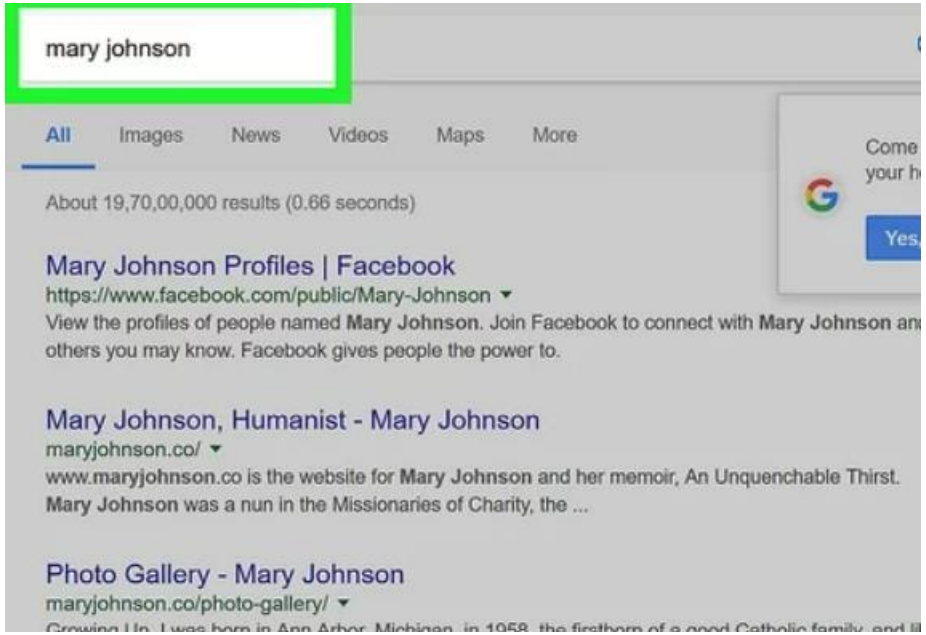
العلامات الدالة على اختراق إلكتروني



3- ابحث عن المزيد من البرامج الضارة التي يُضيفها المخترقون إلى أجهزة الكمبيوتر. فيما يلي بعض الاحتمالات الإضافية لما يمكن أن تراه على جهازك في حالة تعرضك للاختراق:

تستقبل رسائل مزيفة تخبرك بوجود فيروسات على الكمبيوتر. إما أنك تمتلك برمجية للحماية من الفيروسات على الكمبيوتر أو لا؛ في الحالة الأخيرة سوف تظهر لك هذه الرسائل لإخبارك كذبًا عن وجود فيروسات قادرة على إتلاف محتويات الجهاز، أما في الحالة الأولى فالمفترض أنك تعرف شكل رسائل البرنامج المضاد للفيروسات، لذلك انتبه في حالة كان شكل الرسائل مختلفًا عما تعتاد عليه. لا تضغط على أي رابط أو تتفاعل مع هذه الرسائل والتي تحاول الاحتيال عليك بهدف تشجيعك على إدخال بياناتك الشخصية أو المالية الخاصة ببطاقة الائتمان وغير ذلك بعد إيهامك أن ذلك سوف يساعدك على التخلص من الفيروسات على الجهاز. انتبه إلى أن المخترق يتحكم بالفعل في الكمبيوتر (اطلع على الأجزاء التالية لمعرفة ما يجب عليك فعله).

العلامات الدالة على اختراق إلكتروني



- تظهر شرائط أدوات إضافية في متصفح الإنترنت، وربما تحمل رسائل تدعي مساعدتك! يجب أن يوجد شريط أدوات واحد فقط أو الشرائط التي قمت بتثبيتها بنفسك. اشعر بالشك في حالة ظهر لك أي قوائم أو شرائط إضافية.
- تظهر لك نوافذ منبثقة عشوائية ومتكررة على الكمبيوتر. تحتاج إلى معرفة البرنامج الذي يتسبب في هذا الأمر والتخلص منه.
- لا يعمل برنامج مكافحة الفيروسات والبرامج الضارة ويبدو أنه غير متصل. قد يتم إيقاف إمكانية استخدام "مدير المهام" أو "محرر سجل النظام".
- يصل إلى الأفراد الموجودين في قائمتك البريدية رسائل مزيفة وتحمل روابط ضارة.
- تفقد أموال من حسابك البنكي أو تصلك فواتير دفع لمشتريات إلكترونية لم تشرها من الأساس.

العلامات الدالة على اختراق إلكتروني

4- إذا كنت ببساطة لا تملك أي تحكم فيما يحدث على الكمبيوتر، توقع بنسبة كبيرة أنك ضحية لعملية اختراق.

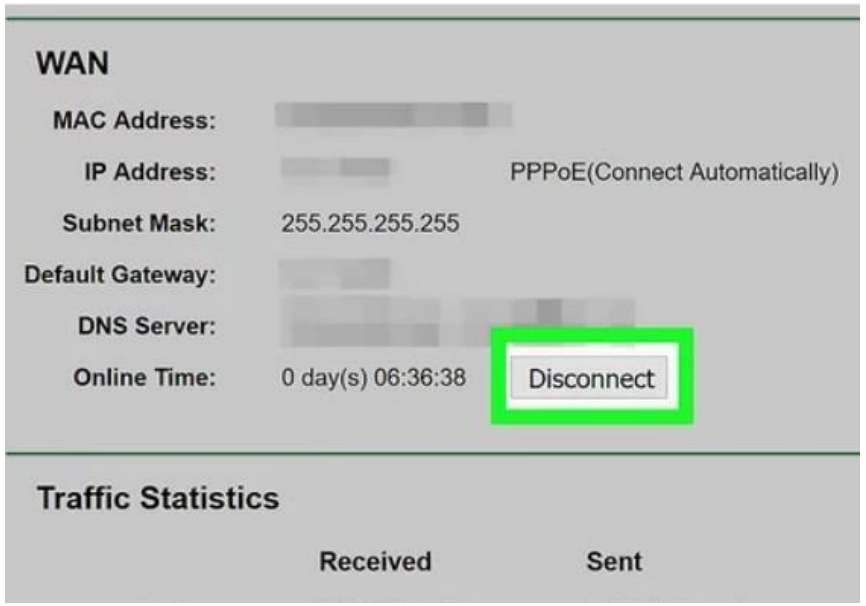
قد تجد في بعض الحالات أن مؤشر الفأرة يتحرك على الشاشة من تلقاء نفسه وينفذ أوامر لم توجهها له على الإطلاق، ويكون ذلك إشارة مؤكدة على وجود طرف بشري في مكان ما في العالم قد نجح في الوصول إلى داخل الكمبيوتر ويتلاعب بك.

ربما أنك تعرف ما نقصد الحديث حوله في حالة استخدامك لأي من برامج التحكم في أجهزة الكمبيوتر عن بعد أو كنت قد سمحت لأحد العاملين في صيانة الكمبيوتر أن يعمل على إصلاح جهازك عن بعد كذلك. أي حركة تظهر أمامك دون أن تكون أنت المسؤول عنها، فهذه إشارة لا جدال حولها على تعرضك للاختراق.

افحص معلوماتك الشخصية.

ابحث عن نفسك عبر موقع البحث جوجل. هل تجد أي نتائج شخصية لم تنشرها بنفسك من قبل؟ قد لا تظهر هذه النتائج في الحال، لكن إبقاء عينك منتبهة إلى هذا الاحتمال قد يكون بالغ الأهمية لكي تسارع بحماية خصوصيتك في حالة ظهور أي من معلوماتك الشخصية عبر الإنترنت.

ما يجب عليك فعله



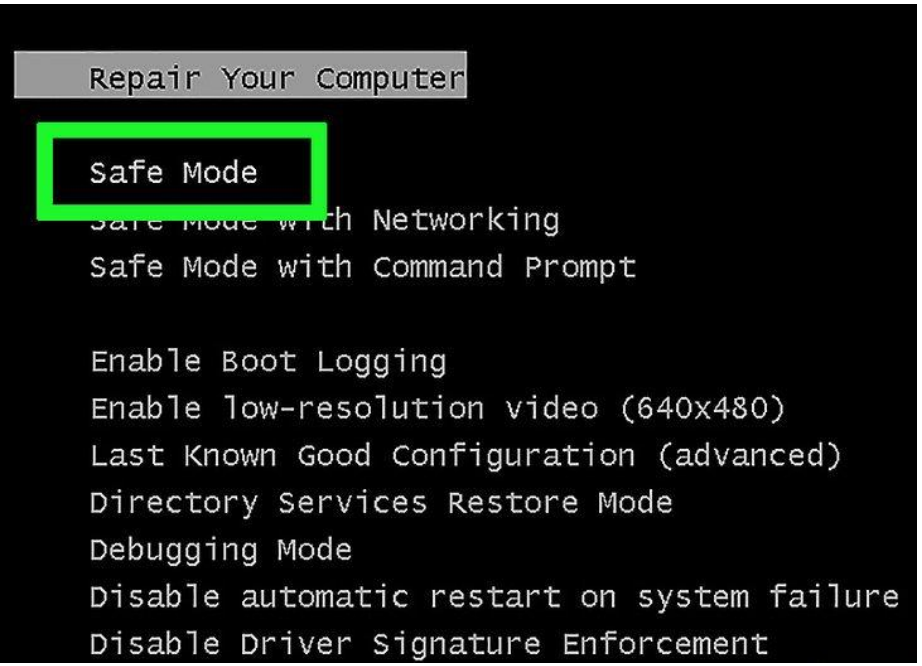
- **اقطع الاتصال بالإنترنت "فورًا".** أفضل شيء يمكنك القيام به هو أن تمنح نفسك فرصة من الوقت للتحري واكتشاف سبب ما يحدث عن طريق قطع الإنترنت في الحال. الإنترنت هو الوسيلة الوحيدة التي يقدر المخترق من خلالها على الوصول إلى الكمبيوتر، وبقطعك للاتصال أنت تحرر جهازك من الوقوع تحت تصرفه.

انزع سلك الراوتر الموصل للإنترنت من المقبس لكي تضمن نهائيًا أنه لا يوجد اتصال بالإنترنت.

- اطبع هذه المقالة أو احتفظ بنسخة بي دي إف منها لكي تقدر على مواصلة متابعة التعليمات الواردة بعد قطع الاتصال بالإنترنت.

يمكنك كذلك أن تستمر في قراءتها باستخدام جهاز منفصل لم يتعرض للقرصنة.

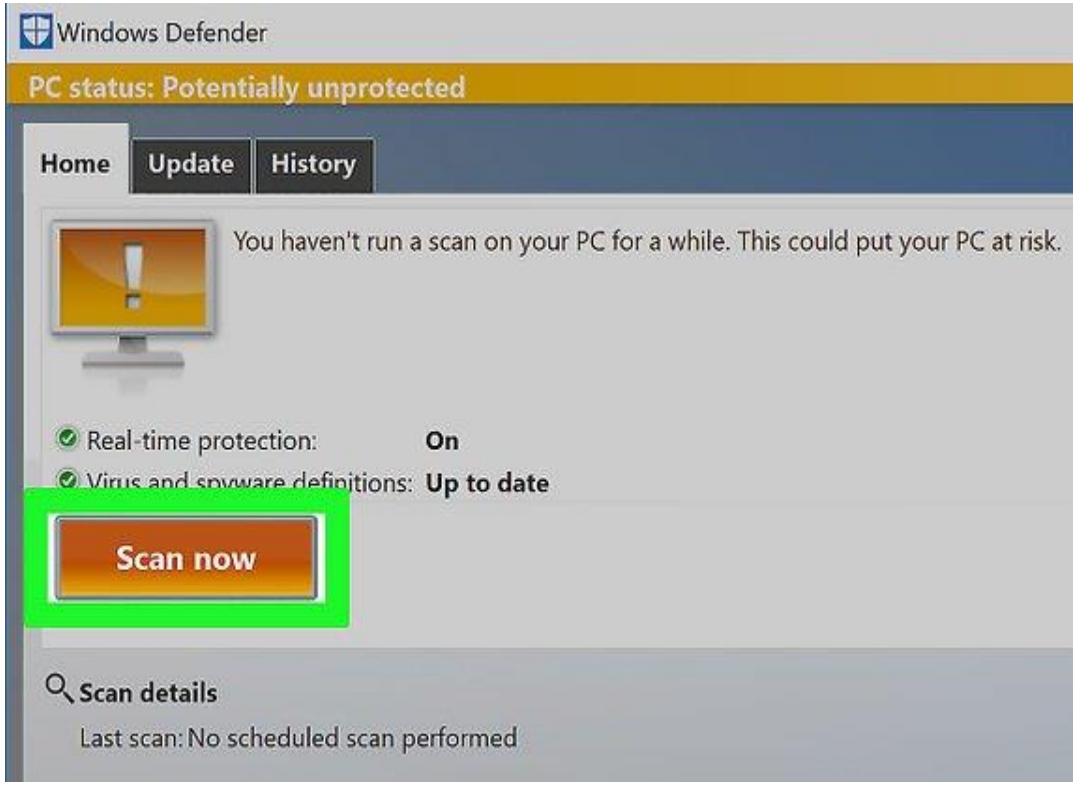
ما يجب عليك فعله



شغِّل الكمبيوتر في الوضعية الآمنة " Safe Mode". تأكد من أن الجهاز غير متصل بالإنترنت نهائيًا واستخدم الوضعية الآمنة من أجل إعادة تشغيله. اطلع على كتيب التعليمات الخاص بنظام التشغيل لمعرفة كيفية الدخول إلى الوضع الآمن.

تأكد من عدم وجود أي برامج جديدة (مثل برامج الوقاية من الفيروسات أو البرمجيات الضارة وغيرهم) أو إذا كانت برامج أو ملفات معينة لا تعمل بطريقة صحيحة. في حالة وجدت أي برنامج غريب مثبت على الجهاز، قم بإزالته في الحال. إذا لم تعرف كيفية القيام بذلك بنفسك، اطلب مساعدة خبير في التعامل مع أجهزة الكمبيوتر أو اتصل بواحدة من خدمات الصيانة لطلب متخصص في الحال.

ما يجب عليك فعله



أجرِ عملية تنظيف للكمبيوتر بواسطة واحدة من برمجيات الوقاية من الفيروسات وبرامج التجسس. من الأمثلة الشائعة: برنامج أفاست أو إيه في جي (النسخة المجانية) أو أفيرا أنتي فيرس... وغيرهم. من جديد، ننصح بأن تحصل على مساعدة خبير في صيانة الكمبيوتر إن كنت لا تعرف ما يمكنك فعله.

إذا لم يحقق لك ما سبق أي شيء، فعلى الأقل، احتفظ بنسخة احتياطية من الملفات المهمة. ثم أجر عملية استعادة كاملة للنظام أو تحديث الكمبيوتر.

تواصل مع البنك والجهات المختصة بحساباتك المالية لإخبارهم بتوقع حدوث عمليات احتيال على حسابك. اسألهم عن النصائح اللازمة لحماية أموالك.

حذر أصدقائك من إمكانية تلقي رسائل بريد إلكتروني مؤذية. أكِّد عليهم أهمية حذف الرسائل التي تصلهم من حساباتك دون فتحها أو الضغط على أي روابط تصلهم عن طريق بريدك الإلكتروني.

العوامل التي تساعدهم على اختراق جهازك ؟

1 - وجود ملف باتش أو تروجان

لا يستطيع الهكر الدخول إلى جهاز الحاسوب إلا عن طريق ملف الباتش أو التروجان الموجود بجهاز الضحية.

ملف الباتش : وهو ملف يجب إرساله للضحية ويجب على الضحية فتحه أيضا حتى يفتح عند الضحيه منفذ (port) ثم يستطيع الهكر اختراقه والتحكم فى جهازه والسيطرة عليه

وأي برنامج باتش يحتوي على 4 أشياء أساسية وهي :

1- ملف الباتش server : وهو ملف يجب إرساله للضحية ويجب على الضحية فتحه أيضا حتى يفتح عنده منفذ (port) ومنه يتم اختراقه..

2- ملف Edit server وهو لوضع إعدادات الباتش أو تغييرها.

3- ملف البرنامج الأساسي Client: وهوالبرنامج الذي يتصل الهاكر من خلاله بالضحية ويتحكم في جهازه..

4- ملفات الـ dll وغيرها: وهي التي تساعد البرنامج على التشغيل ومن دونها لا يعمل البرنامج

العوامل التي تساعدهم على اختراق جهازك ؟

2 - الاتصال بشبكة الإنترنت

لا يستطيع الهاكر الدخول إلى جهاز الضحية إلا عن طريق أتصال الضحية بالأنترنت

فإذا أحس الضحية بإن شخص ما يخترقه يقوم بسرعة بفصل الاتصال بالأنترنت لأن بمجرد فصل الأنترنت و عودة الاتصال به مرة أخرى يتغير IP address الخاص بك

فمثلاً

إذا كان رقمك 212.123.123.200 بعد فصل الأنترنت و العودة يتغير ليصبح كالاتي 212.123.123.366
لاحظ التغير في الجزء الأخير من 200 الى 366

العوامل التي تساعدهم على اختراق جهازك ؟

3- برنامج التجسس

يستطيع الهاكر الدخول إلى جهاز الضحية عن طريق استخدام بعض البرامج التي تساعده على الاختراق و من أشهرها:

BO Client - BusScong - Girl Friend - Net Bus 1.7 - Net Bus Haxporg - Net Buster - Web Cracker 4 Hackers Utility - and Server

ويوجد بعض البرامج الحديثة التي نزلت ولا ترى من قبل برامج الحماية من الفيروسات هي:

NOVA OptixPro CIA122b BEAST

و غيرها من البرامج الشهيرة و طبعا البرامج التي صممها الهاكر بأنفسهم على لغة برمجة معينة فبالتالي يمكنهم ان يضيفوا عليها أشياء لا ترى من قبل برامج الحماية.

كيف يتمكن الهاكر من الدخول إلى جهازك ؟

عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس وهو " الباتش أو التروجان" فإنه على الفور يقوم بفتح بورت (port) منفذ داخل جهازك فيستطيع كل من لديه برنامج تجسس أن يقتحم جهازك من خلال هذا الملف الذي يقوم بفتح منطقة أشبه بالنافذة السرية التي يدخل منها اللصوص وهم الهاكرز!!

عند الإصابة بملف الباتش يحدث التالي :

يتجه إلى ملف تسجيل النظام (registry) حيث ان النظام في كل مرة عندما تقوم بتشغيل الويندوز يقوم الويندوز بتشغيل البرامج المساعدة في ملف تسجيل النظام مثل برامج الفيروسات وغيرها .

1. يقوم بفتح ملف اتصال داخل الجهاز المصاب تمكن برنامج الهاكر من الدخول إلى جهازك و التجسس عليه.
2. يقوم بعملية التجسس وذلك بتسجيل كل ما يحدث أو عمل أشياء أخرى على حسب ما يريد.

و هذا يعني ان الجهاز إذا أصيب فإنه يصبح مهيأ للاختراق.

ما هو رقم الآي بي أدرس : (IP (internet protocol

هو العنوان الخاص بكل مستخدم لشبكة الإنترنت أي أنه الرقم الذي يُعَّرف مكان الكمبيوتر أثناء تصفح شبكة الإنترنت

وهو يتكون من ٤ أرقام وكل جزء منها يشير إلى عنوان معين فأحدها يشير إلى عنوان البلد والتالي يشير إلى عنوان

الشركة الموزعة والثالث إلى المؤسسة المستخدمة والرابع هو المستخدم..

ورقم الآي بي متغير وغير ثابت فهو يتغير مع كل دخول إلى الإنترنت .. بمعنى آخر لنفرض أنك اتصلت بالانترنت

ونظرت إلى رقم الآي بي الخاص بك فوجدت أنه :212.123.123.200

ثم خرجت من الانترنت أو أقفلت الاتصال ثم عاودت الاتصال بعد عدة دقائق فإن الرقم يتغير ليصبح

كالتالي: 212.123.123.366

لاحظ التغير في الأرقام الأخيرة : الرقم 200أصبح 366

كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟

الطريقة الأولى:

أن يصلك ملف التجسس من خلال شخص عبر المحادثة أو الشات وهي أن يرسل لك أحد الهاكر صورة أو ملف يحتوي على الباتش أو التروجان !

ولابد أن تعلم أنه بإمكان الهاكر أن يغرز الباتش في صورة أو ملف فلا تستطيع معرفته إلا باستخدام برنامج كشف الباتش أو الفيروسات حيث تشاهد الصورة أو الملف بشكل طبيعي ولا تعلم أنه يحتوي على باتش أو فيروس ربما يجعل جهازك عبارة عن شوارع يدخلها الهاكر والمتطفلون!

الطريقة الثانية:

أن يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل فتقوم بتنزيل الملف المرفق مع الرسالة ومن ثم فتحه وأنت لا تعلم أنه سيجعل الجميع يدخلون إلى جهازك ويتطفلون عليك..

كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟

الطريقة الثالثة:

أن يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل ويقول أدخل على الرابط التالي فتقوم بالدخول ومن ثم الإصابة بملف الباتش.

الطريقة الرابعة:

إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الغير أخلاقية أو المواقع التي تساعد على تعليم التجسس !

الطريقة الخامسة:

الدخول إلى مواقع مشبوهة مثل المواقع الغير أخلاقية حيث أنه بمجرد دخولك إلى هذه المواقع فإنه يتم تنزيل الملف في جهازك بواسطة كوكيز لا تدري عنها حيث يقوم أصحاب مثل هذه المواقع بتفخيخ الصفحات فعندما يرغب أحد الزوار في الدخول إلى هذه الصفحات تقوم صفحات الموقع بإصدار أمر بتنزيل ملف التجسس في جهازك!

!!

كيف يختار الهاكر الجهاز الذي يود اختراقه ؟

بشكل عام لا يستطيع الهاكر العادي من اختيار كمبيوتر بعينه لاختراقه إلا إذا كان يعرف رقم الآي بي أدرس الخاص به

كما ذكرنا سابقاً فإنه يقوم بإدخال رقم الآي بي أدرس الخاص بكمبيوتر الضحية في برنامج التجسس ومن ثم إصدار أمر الدخول إلى الجهاز المطلوب!!

وأغلب المخترقين يقومون باستخدام برنامج مثل (IP Scan) أو كاشف رقم الآي بي وهو برنامج يقوم الهاكر باستخدامه للحصول على أرقام الآي بي التي تتعلق بالأجهزة المضروبة التي تحتوي على ملف التجسس (الباتش)

حيث يتم تشغيل البرنامج ثم يقوم المخترق بوضع أرقام آي بي افتراضيه .. أي أنه يقوم بوضع رقمين مختلفين فيطلب من الجهاز البحث بينهما

ما هي أهم الأشياء التي يبحث عنها الهاكرز ؟

1. الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية.
2. الحصول على معلومات أو صور شخصية بدافع الابتزاز لأغراض مالية أو انحرافية كتهديد بعض الفتيات بنشر صورهن على الإنترنت إذا لم يستجبن لمطالب انحرافية أو مالية!!
3. الحصول على ملفات جميلة مثل ملفات الأركامكس أو الباور بوينت أو الأصوات أو الصور أو...
4. إثبات القدرة على الاختراق ومواجهة العقبات وفرصة للافتخار بتحقيق نصر في حال دخول الهاكر على أحد الأجهزة أو الأنظمة المعلوماتية..
5. الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة اسم البريد الإلكتروني بأكمله!!
6. الحصول على الرمز السري لأحد المواقع بهدف تدميره أو التغيير في محتوياته..
7. الانتقام من أحد الأشخاص وتدمير جهازه بهدف قهره أو إذلاله

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

1- استخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي..

2- التأكد من تحديث الانتي فيروس كل أسبوع على الأقل (شركة نورتون تطرح تحديث كل يوم أو يومين)

3- التأكد من أن Firewall على وضعية on

4- وضع Anti-Virusجيد و انا انصح بوضع انتي فيرس الشمسية (Avira)

5- لا تظل مدة طويلة متصل بالشبكة بحيث لو ان احد قام بالدخول عليك لا يستطيع أن يخرب فى جهازك فعند خروجك و دخولك مره اخرى للشبكة يغير آخر رقم من الاي بي.

6 -لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاماً وصوراً لا أخلاقية لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

7- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا.

8 -عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe)أو أن تكون ملفات من ذوي الامتدادين مثل (xxx.pif.jpg)أو (.bat أو .dll أو.com)

وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبب الأذى والمشاكل لك..

9 -عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية....

10 -قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت وسوف نشرحها

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

11- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق.

12 -حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق ويفضل أن تكون كلمة السر أرقام وحروف ورموز يصعب تخمينها .

13- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.

14- لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره.

15- قم بمسح cookies أول بأول من جهازك هي عبارة عن ملفات يرسلها الموقع لمتصفحك

و هي عبارة عن ملف مكتوب لا يستطيع أي موقع قراءته غير هذا الموقع و قد يكون به كلمات سر موقع أو اشتراك... وهي مزعجه في بعض الأحيان حيث أنها تسجل كل المواقع التي دخلتها و كل الصفحات التي شاهدتها و مدة مشاهدة كل صفحه....

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

* ويمكن مسح الكوكيز عن طريق الذهاب المجلد الخاص بها و حذف الملفات التي به C:\WINDOWS\Cookies و حذف الملفات التي توجد داخل هذا المجلد

* أو من قائمة Start نختار Run ونكتب فيها Cookies ثم OK ستظهر نافذة نمحو كل ما فيها

16- لا تخزن كلمات المرور أو كلمات سر على جهازك مثل كلمة المرور لاشتراكك في الانترنت أو البريد الكتروني أو .....

17- إذا لاحظت حدوث اي شيء غريب مثل خلل في اي برامج أو خروج و دخول السي دي افصل الاتصال بالانترنت فورا و تأكد من نظافة الجهاز.

18- أغلق خاصية الاكمال التلقائي من انترنت اكسبلورر .. ولا تسمح بحفظ كلمات المرور في النماذج .

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

19- لا تدخل بريدك أو أيّ من معلوماتك الخاصة من مقاهي الانترنت نهائيا .. فهناك برامج تعمل بشكل مخفي تحفظ جميع النماذج التي تقوم بتعبئتها دون أن تشعر.

20- غيّر كلمات مرورك بين فترة وأخرى .. وينصح أن تكون الكلمة مكونة من حروف وأرقام كثيرة يصعب تخمينها ، لأن هناك برامج تقوم بتجريب الآلاف من كلمات المرور وتعمل مسح على مدار الساعة .. فيدخل المخترق اسم المستخدم للبرنامج ويطلب منه تخمين كلمة المرور ..

* فإذا كانت كلمة المرور سهلة مثل هذه 12345 فسوف يحصل عليها في وقت قياسي

* ولكن إذا كانت كلمة المرور صعبة مثل Rhjju665dTpl,Q:4#6;/.gf9 فسوف يكون من الصعب جدا أن يكتشفها البرنامج بالتخمين ولو بعد 100 سنة وتزداد الصعوبة أكثر إذا أضيف في كلمة المرور أحرف أخرى باللغة العربية في المواقع التي تسمح بذلك.

21- لا تستخدم كلمة مرور موحّدة .. بل اجعل كلمة مرور بريدك تختلف عن معرفك بالساحة .. وأيضا تختلف عن معرفك في المنتديات الأخرى .. ولو استطعت أن تجعل لكل منتدى أو بريد كلمة مرور مختلفة فافعل .. وضع جدولا لكلمات المرور على مكتبك وليس في جهازك .

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

22- احذر من مواقع الكراكات والسيريالات والمواقع غير الموثوقة ففيها برامج يتم تحميلها في الخلفية أثناء تصفح الموقع .. وهي تتحدّث بشكل مستمر .. وأحيانا تفشل برامج السباي وير في مقاومتها أو القضاء عليها .. وكذلك عند تركيب كراك لبرنامج فكثير من هذه الكراكات يحتوي على باتش يمكن أن يكون عند تشغيله ثغرة خطيرة في جهازك.

23- للعلم مواقع المراسلة التي ظهرت مؤخرا وشارك فيها كثير من الأعضاء .. من السهل جدا جدا للعاملين بتلك المواقع .. الاطلاع على محتويات الرسائل الموجودة بها .. ولذا إذا استخدمتها فكن على حذر .. فالرسائل الواردة إليك والمرسلة منك عن طريقها مكشوفة بنسبة 100%!!

24- على أسوأ الاحتمالات لا تترك بيانات أو ملفات أو مستندات خاصة بك في بريدك الالكتروني .. بل بادر بمسحها أو الاحتفاظ بها في جهازك .. وأيضا يفضّل أن تحفظ ملفاتك الشخصية الخاصة والتي لا ترغب أن يطّلع عليها أحد في فلاش ديسك أو هارديسك خارجي .. وتقوم بفصلها عند الاتصال بالانترنت ..

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

25- ما يقوله جوجل صحيح .....فإذا قمت بعمل بحث على موقع ووجدت جوجل يحذرك من هذا الموقع لا تدخل على هذا الموقع لأنه قد يضر بجهازك.....فقد يحتوى على برمجيات خبيثة وسوف تنزل على جهازك من دون أن تشعر وسوف تكون بذلك ضحية لأى هاكر.

26- المواقع الموجودة فى رسايل الـ spamمواقع خطيرة...يمكن أن تحتوى على برمجيات خبيثة.

27- الأبتعاد عن برنامجى ICQ و IRC لأنهم يسهلوا عملية الاختراق.

28- انصح كل عضو ان يكون له 3 ايميلات واحد منها مخصص للشبكة و يفضل ان يكون على الجي ميل حتى لا يستخدم في الماسينجرات و ايميل اخر للماسينجر و ايميل للمراسلات الخاصة حتى ان تم سرقة باسورد ايميل الماسينجر لا يكون هناك ضرر معين و ان يكون الايميل المخصص للشبكة بأي اسم غير اسمك الحقيقي كما انصح الجميع عند ارسال ايميلات لعدة اصدقاء ان يتم وضع

الايميلات في خانة BCC حتى لا يرى الجميع ايميلات الاخرين و تكون فرصة ثمينة لمن يخترق احدى هذه الايميلات.

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

29- جميع الأجهزة المتصلة بالشبكة عرضة للإصابة بالفيروسات في حالة مشاركة الملفات فيما بينها

أو في حالة مشاركة الاتصال بالإنترنت بينها. لذلك يجب تعطيل وظيفة تبادل الملفات والطابعات وتفعيل الدخول إلى الجهاز بكلمة سر حتى يتم تجنب المخاطر إلى حد كبير..

30- المتصفح الذى تقوم بأستخدامه سواء انترنت اكسبلورر او فاير فوكس او غيره ....لابد أن يكون أحدث نسخة موجودة

31- تفريغ قائمة my recent document لأنها أول ما يلهث إليه لص المعلومات هو آخر ملفات تعاملت معها مؤخراً وما بها من معلومات فيبحث عنها على القائمة سالفة الذكر

* لتفريغ هذه القائمة ننقر بزر الماوس الأيمن على أي مكان خال فوق شريط المهام أسفل الديسك توب ثم نختار Properties ثم start menu ثم نضغط زر customize ثم advanced ثم زر clear list ثم نضغط ok مرتين.

أهم الاحتياطات التي يجب اتخاذها للحماية من الاختراق ؟

32- جميع مراسلات الشبكة تتم من خلال ايميل الشبكة ali@paldf.net او

webmaster@paldf.net لذلك في حال وصول رسالة على ايملك من غير هذين الايميل اهمالها

وعدم التجاوب معها.

كيف تعرف ان الصورة المرسلة لك ملغمة "أى مدموج فيها باتش"؟

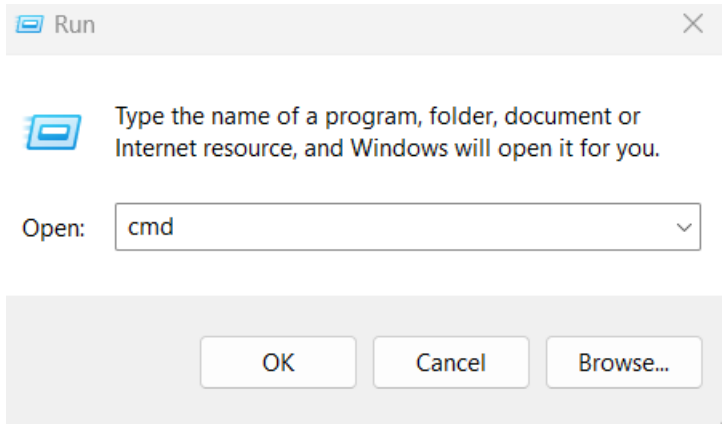
اولاً لابد أن نعرف بوجود صيغ تنفيذية وصيغ غير تنفيذية

فالصورة التي تكون صيغتها غير تنفيذية مثل bmb , png , jpg , jpeg , gif

لكن إذا وجدنا صورة صيغتها مثلا dll , cox , com , exe , bat , pif , vbs , dif , shs , scr

فهذه صيغ تنفيذية ومنها نعرف أنها ليست صورة ...وأنها تروجان ومدموج معها صورة

كيف تعرف ان جهازك مخترق



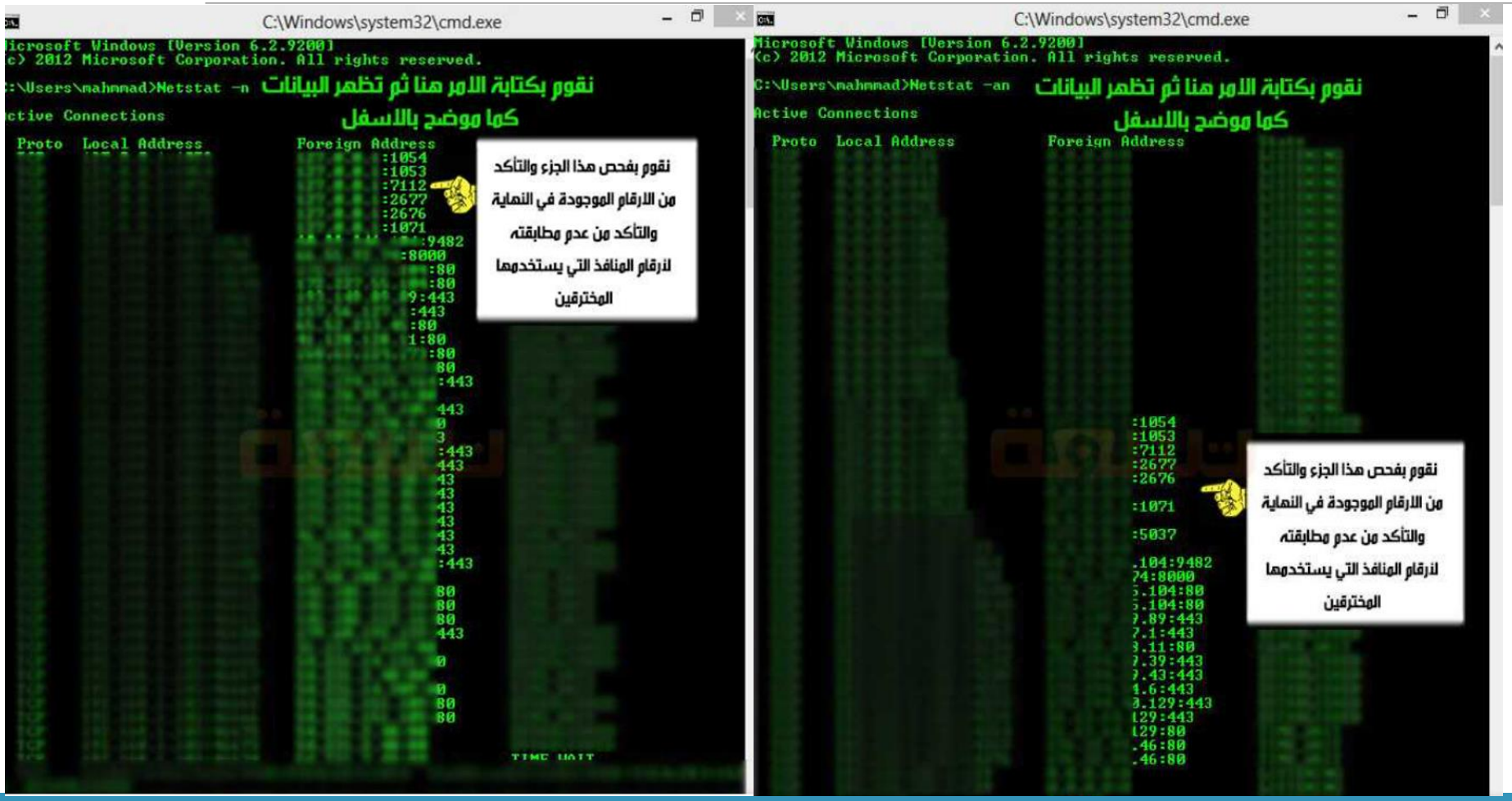
1- اذهب الى نافذة الأوامر Run ثم اكتب cmd تنبثق لديك نافذة سوداء : اكتب فيها الأمر netstat –n تظهر ليك مجموعة من ال IP Address كما في الصورة

اذا طابق احد الأرقام في قائمة: Foreign Address القائمة التالية تعرف عندها ان جهازك مخترق:

أشهر ارقام المنافذ التي يمكن ان تمثل خطورة على جهازك ان وجدت :

3460,1826,6200,6300,3646,777,888,288,83,5015,197 192 ,137,110,113,119,121,123,133,137,138,139,81

كيف تعرف ان جهازك مخترق



2- اذهب الى نافذة الأوامر Run ثم اكتب cmd تنبثق لديك نافذة سوداء : اكتب فيها الأمر netstat –an تظهر ليك مجموعة من ال IP Address كما في الصورة

وهذا الأمر يظهر المزيد من المنافذ التي لا تظهر في الأمر السابق

كيف تعرف ان جهازك مخترق

نقوم بكتابة الامر التالي (System.ini) بداخل نافذة التشغيل (Run) ثم نقوم بالضغط على موافق (Ok).

الان نلاحظ ظهور نافذة المفكرة (Notepad) وبها بعض البيانات وللتأكد من إذا كان الجهاز مخترق ام لا نقوم بالتدقيق في الملف الظاهر امامنا والتأكد من الخطوتين التاليتين:

التأكد من عدم وجود الرمز الموجود بين القوسين (***) بجوار الكلمة timer=timer.drv لأن ان وجدت فهذا يدل ان الجهاز مخترق ام ان لم نجدها فهذا يدل ان الجهاز سليم.

في الأربع أسطر الموجودين في اول الملف النصي نتأكد من وجود الكلمة (FON) فإذا وجدناها يكون في تلك الحالة جهازك غير مخترق اما إذا وجدنا كلمة (BD) بدلا من كلمة (FON) ففي تلك الحالة يكون جهازك مخترق.

طرق إزالة ملفات التجسس من جهازك

الطريقة الأولى: نقوم بالذهاب الى جهاز الكمبيوتر (My Computer) ثم الى إدارة (Mange).

بعد فتحة نافذة إدارة الكمبيوتر (computer management) نقوم بالذهاب الى مشاركة الملفات (Shared Folder) والتأكد من عم وجود أي جلسات نشطة داخل الملف (Sessions) وان وجدت أي جلسات نشطة نقوم بإيقافها وإزالتها فورا.

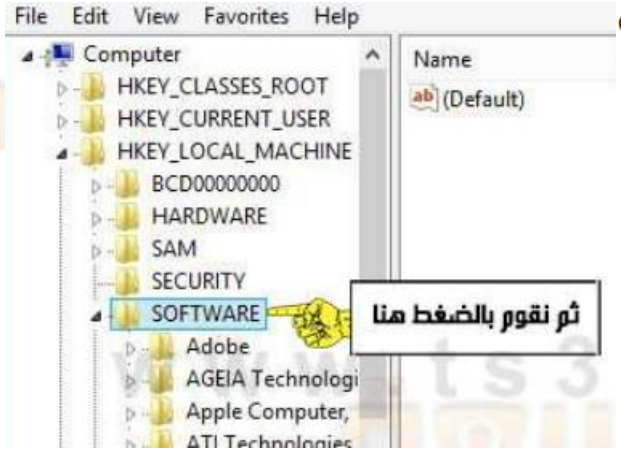
طرق إزالة ملفات التجسس من جهازك

الطريقة الثانية: نقوم بفتح نافذة التشغيل (Run) ونقوم بكتابة الامر التالي (Regedit) من اجل تشغيل محرر التسجيل (registry Editor) ثم نقوم بالضغط على موافق (Ok).

بعد تشغيل محرر التسجيل (registry Editor) نقوم بالذهاب الى الخيارات كما موضح في الترتيب التالي.

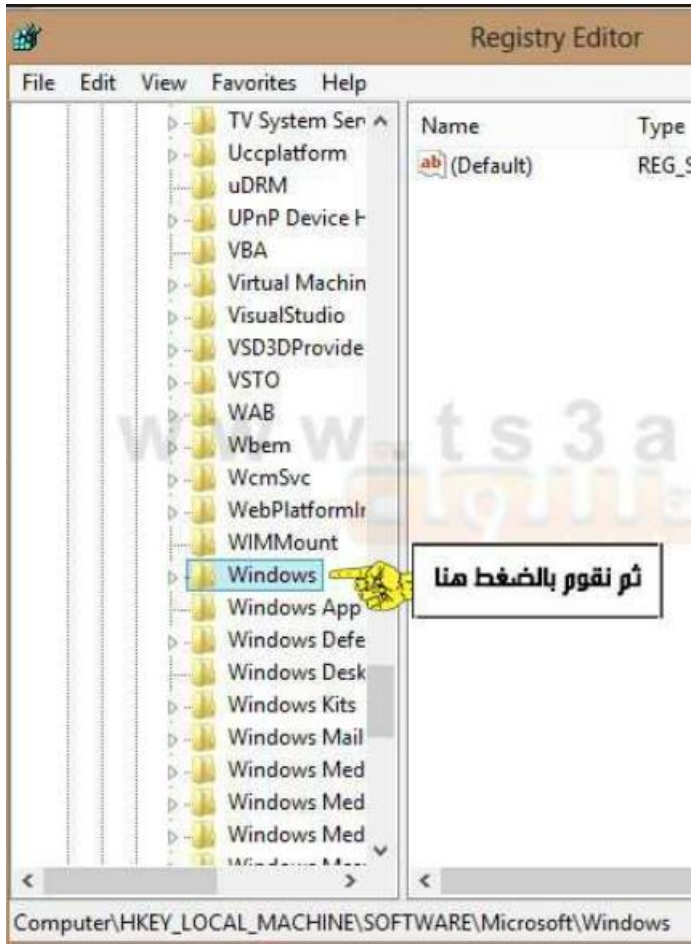
-نقوم بالضغط على (HKEY_LOCAL_MACHINE). ثم نقوم بالضغط على الملف (SOFTWARE)

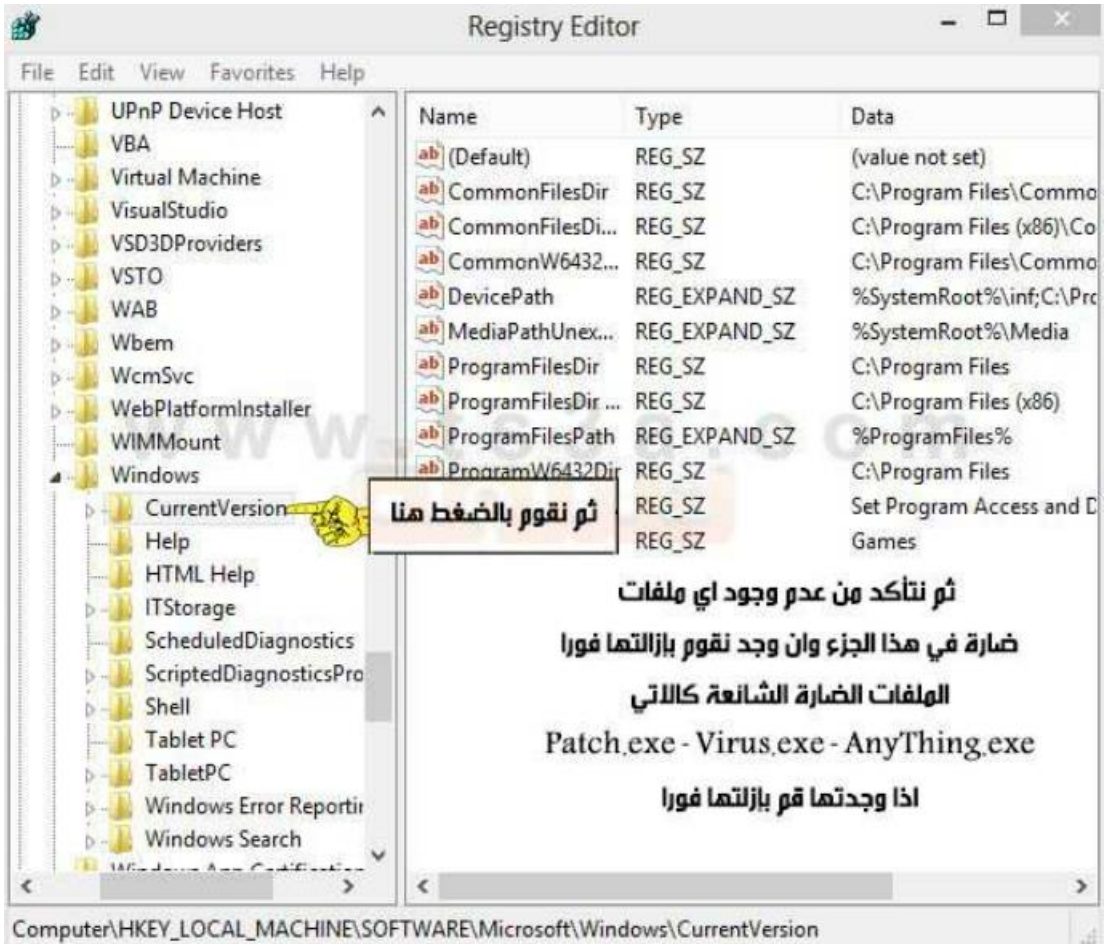
ثم نقوم بالضغط على الملف (Microsoft) ثم نقوم بالضغط على الملف (Windows)



ثم نقوم بالضغط على الملف (Current Version) ونقوم بالنظر للملفات التي يحتويه هذا الملف وإذا وجد أي ملف بصيغة (EXE) لا يتم استخدامه من قبل النظام نقوم بإزالته فورا.

طرق إزالة ملفات التجسس من جهازك





طرق إزالة ملفات التجسس من جهازك

الطريقة الثالثة

نقوم بتشغيل نافذة الأوامر السريعة (cmd) والتي تعرفنا في اول الشرح كيف يتم فتحها ثم نقوم بكتابة الامر التالي (/cd) ثم نقوم بالضغط على زرد الادخال (Enter)

نقوم الان بكتابة الامر التالي (dir patch) لاستعراض ملفات الباتش الموجودة في جهازك وهناك إجراءان يجب اتخاذهم كل اجراء مرتبط بالنتيجة التي ستظهر.

فإذا ظهرت النتيجة التالية (File Not Found) فهذا يدل ان جهازك سليم ولا يحتوي على أي باتش.

لكن إذا ظهرت أي ملفات نقوم بكتابة الامر التالي (windowsdeletepatch) وهذا الامر سيعمل على إزالة ملفات الباتش من جهازك بصورة نهائية.

الأكاديمية العربية الدولية
Arab International Academy

طرق إزالة ملفات التجسس من جهازك

أشهر برامج الحماية – أفكار مفيدة

BlackICE Defender v2.5 co

•عندما تخرج من المنزل، تأكد من فصل اتصال الإنترنت وقطع الكهرباء عن جهاز الراوتر.

•تأكد دائمًا من صنع نسخ احتياطية من ملفات النظام أو الملفات الهامة على القرص الصلب.

•للحفاظ على نظام التشغيل قبل عملية الاختراق، استخدم برنامج استرجاع النظام (.Back-Up)

•الوقاية دائمًا خير من العلاج.

Norton Internet Security 2001 v 2.5 Family Edition

•اصنع نسخ احتياطية من الملفات المهمة مثل صور العائلة والمستندات الخاصة بالعمل والملفات التي لن تقدر أبدًا على الوصول لها إذا ضاعت. استخدم فلاشة يو إس بي مشفرة واحتفظ بها في مكان آمن. من الحلول الأخرى الذكية للغاية أن تعتمد على تخزين الملفات على التخزين السحابي (الكلاود)" مثل برامج "جوجل درايف" أو "وان درايف" أو "دروبوكس".

Tiny Personal Firewall 2.0.14

Zone alarm

Intruder Alert '99

•أغلق الإعدادات الخاصة بالموقع الجغرافي تمامًا. تصعب هذه الخطوة من إمكانية وصول أي مقرصن إلى مكانك، بالتزامن مع استخدامك لشبكة خاصة افتراضية قوية ((VPN، مثل: (برنامج S F-Secure Freedomeاحرص كذلك على عدم مشاركة موقعك من خلال شبكات التواصل الاجتماعي، مثل: فيسبوك وإنستجرام، سواء من خلال صفحة البيانات الشخصية أو ذكر موقعك في أثناء نشر تحديثات جديدة.

أشهربرامج مقاومة الفيروسات - تحذيرات

Mcafee

Norton Anti-Virus

Pc-cillin

AntiViral Toolkit Pro (AVP) Gold

AntiViral

Norton Anti-Virus 2001

Cleaner V.3.2

Avira personnel

•إذا كانت بعض البرامج أو الملفات لا تعمل بشكل صحيح أو لا تُفتح من الأساس، فلن يكون أمامك سوف تثبيت نسخة نظام تشغيل جديدة أو على الأقل استعادتها بتاريخ قديم، بشرط ألا يكون المقرصن قد تلاعب بدوره بالنسخ الاحتياطية من نظام التشغيل.

•يجب أن تسارع بعلاج الأمر وإلا قد يتحول جهازك لمصدر لتوزيع الهجمات على الضحايا الآخرين، سواء كانوا شبكات أو أجهزة كمبيوتر، والاستمرار في المزيد من الأنشطة غير القانونية.

•إذا لم يتم فحص ومعالجة الجهاز، فقد يسوء الوضع كثيرًا ويصبح الكمبيوتر عديم الاستخدام. قد تضطر إلى إعادة تثبيت نسخة جديدة من نظام التشغيل أو شراء كمبيوتر جديد كليًا.

توخي الحذر الشديد من الجميع في التعامل مع ما يلي

اولا E-MAIL:

*يجب الحرص الشديد على كلمة السر وتغيرها من فترة الى اخرى

*عدم فتح الرسائل اذا لم تعرف مضمونها او اذا لم تعرف عنوان الشخص المرسل

* ايضا تجنب اعطاء عنوانك البريدي لاي شخص او شركة غير معروفين لديك

*بعض الرسائل القادمة الى البريد الالكتروني تاتي بعناوين مغرية ومشوقة لفتح هذة الرسائل ولكن لا تقوم بفتحها بل قم مباشرة بالغاءها وكما لاحظت من ان كثير من برامج الاختراق والفيروسات تستطيع الدخول الى جهازك عن طريق البريد الالكتروني

* ايضا قم دائما بتنظيف بريدك من الرسائل القديمه والغير مهمة.

توخي الحذر الشديد من الجميع في التعامل مع ما يلي

ثانيا : GAMES

يجب الحرص ايضا من التعامل من العاب الكمبيوتر خاصة التي تحتاج إلى تشات من الموقع او التي تكون تحت عنواين مشبوهة مثل وألعاب اليانصيب للحظ السعيد وغيرها من الالعاب

ثالثا : SCREEN SAVERS

احرص ايضا من تحميل الـ SCREEN SAVERSمن الانترنت لانه قد يكون مرفق معها بعض الفيروسات او برامج الاختراق . ايضافة الى انها قد تؤثر على جهازك فبعض المشاكل التي تواجة اجهزتنا يكون سببها هو الـ SCREEN SAVERS

توخي الحذر الشديد من الجميع في التعامل مع ما يلي

رابعا **SOFTWARES**

لا تقوم بتحميل برامج عن طريق الانترنت من شركات ضعيفة او غير معروفة في عالم الكمبيوتر

ايضا حاول دائما تحميل البرامج خارج ال سي درايف اي باستخدام CD-Writerاو باستخدام

Zip-drive

خامسا **chat**

تجنب التعامل مع برامج المحادثة الأتيه وايضا يفضل حذفها من الجهاز واذكر منها :-

ICQ ------ MIRC ------ FREETEL ------ NETMEETING ------ irc

شكراً لحضوركم

آمل ان تكونوا قد حققتم الفائدة