**14 method to make your malware clean**

بسم الله اليوم بشرح لكم كيف تسوي malware بطريقة تصعب على Anti vitus و اي محلل مالوير يعرف وش قاعد تسوي

**وش يعني sandbox**

كثير من برامج الحماية تشغل الملفات في نظام وهمي عشان تشوف هل الملف يسوي شي ضار او لا و بنفس الوقت محللين المالوير يسوونها عشان ما يتضرر النظام الاساسي و كثير يستخدمون Virtualbox



Virtualbox

**وش الفائدة اننا نكشف sandbox**

مثل ماقلنا فوق برامج الحماية تشغل الملف حقك في نظام وهمي (sandbox) عشان تشوف اذا كان ضار او لا طبعا هذي مو الطريقة الوحيدة بس هذي احد الطرق ف اذا قدرنا نعرف ان المالوير حقنا شغال في نظام وهمي نقدر مانسوي شي ضار عشان يعتبر برنامجنا برنامج سليم

**طرق كشف sandbox**

فيه طرق كثير مرة بشرح بعض منها

بما ان النظام الوهمي مواردة محدودة راح نستفيد من الشي ذا وش يعني مواردة محدودة؟ يعني النظام يكون فيه 4 قيقا رام مثلا ف يعتبر ضعيف

**RAM**

في النظام الوهمي نقول انه يحتوي على 1 قيقا رام راح نخلي البرنامج حقنا يتحقق اذا النظام اللي شغال عليه اكثر من 4 قيقا رام او لا بستخدم C# لأنها مشهوره في كتابه المالوير و الكود سهل فهمه

Text

Description automatically generated

بعد مايشيك اذا الرام اقل من 4 يسكر البرامج و مايسوي شي يفضل انك ماتسكره بس تغير طريقة تشغيله

**CORES**

مثل الطريقة اللي فوق الجهاز مواردة بسيطة بنسوي تحقق Cores بالجهاز و اذا كانت قليل نسكر

Text

Description automatically generated

**Disk**

الانظكة الوهمية مساحتها تجي قليلة راح نستغل الشي هذا و نشيك

Text

Description automatically generated

**network**

لما يشغل برنامج الحماية الملف حقنا مايكون متصل بالانترنت و بنفس الوقت اذا بيحلل شخص المالوير يفصله عن الانترنت راح نستفيد من الشي هذا و نشوف هل فيه اتصال بالنت او لا بس هل هذا كافي؟ لا ممكن محلل المالوير يستخدم [Fakenet](https://github.com/mandiant/flare-fakenet-ng) بحيث انه يوهمنا اننا في نظام حقيقي و متصل بالشبكة بهذي الحاله ممكن نسوي ريقويست لقوقل و نشوف الريسبونس كم بايت فيه بالطريقة هذي نتأكد اذا كان Fakenet او لا

Text

Description automatically generated

**sleep**

برامج الحماية لما تشغل الملفات تشغلها لمدة معينة عشان ما تستهلك موارد كثير من الجهاز ف مثلا ممكن تشغل الملف 30 ثانية ف ممكن نخلي البرنامج حقنا لا يشتغل لمدة 30 ثانيه و بعدها يشتغل بهذي الطريقة ممكن نتخطى بس برامج الحماية صارت اذكى و صارت تسوي api hooking بحيث لو حطينا sleep لمدة ساعتين مثلا ما تجلس نص ثانية باختصار يتلاعب بوقت sleep حقنا ف ممكن نستفيد من الشي هذا و نشيك عن فعلا مرت ساعتين او لا

Text

Description automatically generated

هنا سوينا sleep لمدة ثانيتين و بعدها تأكدنا هل فعلا مرت ثانيتين او لا

​

**debugger**

كثير من محللين المالوير يستخدم debugger عشان يعرف كيف البرنامج حقنا يشتغل بشكل dynamic ف ممكن نتحقق هل يوجد debugger او لا

Text

Description automatically generated

هذي مو الطريقة الوحيدة اللي نكشف فيها اذا فيه احد يسوي debug لبرنامجنا او لا احد الطرق الاخرى اننا نسوي debug للبرنامج حقنا لأن مستحيل يكون فيه اثنين debugger بنفس الprocess بيصير خطأ

​

**For loop**

مثل ماقلنا مانقدر نسوي sleep ف راح نسوي loop لوقت طويل بحيث تقوم بنفس عمل sleep

Text

Description automatically generated

**message box**

لما يشتغل المالوير في نظام وهمي مايكون فيه مستخدم ف ممكن نستخدم طرق تعلمنا هل فيه مستخدم او لا و منها messagebox

Text

Description automatically generated

احد الطرق الثانية موقع الماوس اذا تغير او لا و اذا انضغط الماوس او لا

**GetTickCount**

و هذي فنكشن تعملنا كم من الوقت النظام شغال ف ممكن نتأكد النظام شغال اكثر من 10 دقايق كمل او غير كذا سكر البرنامج

​

**Recent files**

لما يكون النظام وهمي مايكون فيه ملفات او تكون الملفات في Recent files قليل جدا

Text

Description automatically generated

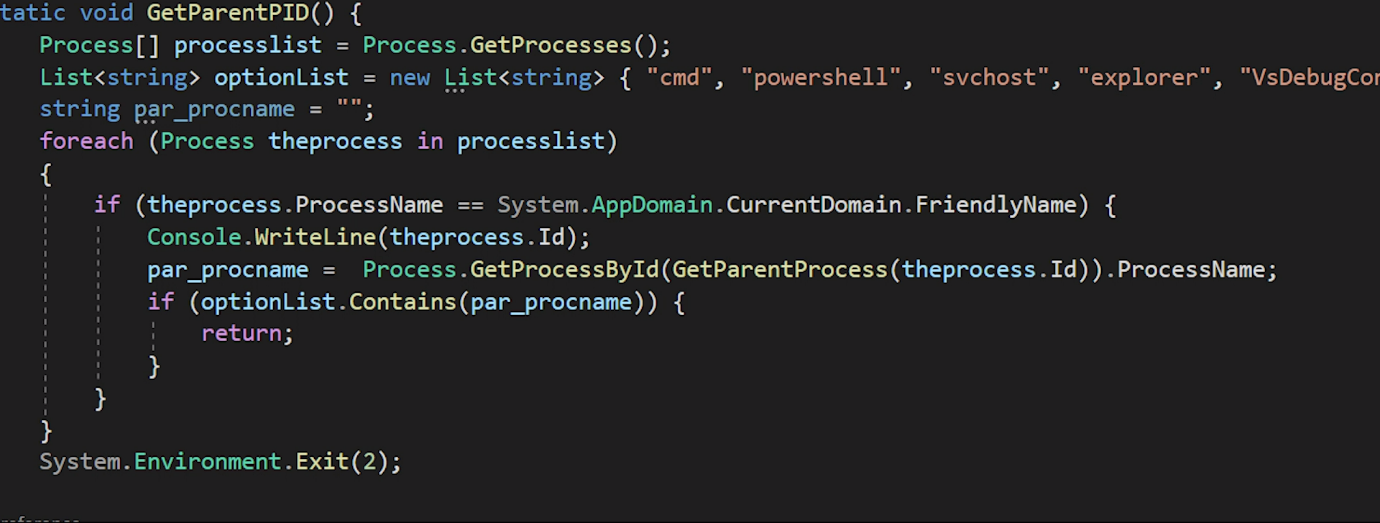
**Services & Processes**

لما يكون النظام وهمي بنلاحظ فيه Services او Processes خاصه في vm ف ممكن نتأكد اذا كانت فيه او لا

​

**ParentPID**

احد الطرق اللي تخلينها نتخطى ال debugger هي ParentPID



بالطريقة هذي اذا الملف اشتغل عن طريقة نشيك ممكن تغيرها ان او ممكن تخليها blacklist

​

**Rename File**

Text

Description automatically generated

اغلب محللين المالوير اذا حمل مالوير او يبي يحلل مالوير يغير اسمه و حنا راح نقارن اسم الملف حقنا بالاسم الاصلي

​

**Mac address**

الانظمة الوهمية يكون لها mac address متعارف بينهم ف ممكن تستخدم الشي هذا عشان تشيك اذا كان يشتغل بنظام وهمي او لا

​

Text

Description automatically generated

​

**Real Example**

Graphical user interface, text, application, email

Description automatically generated

بعد ما رفعنا المالوير اكشفته فقط برنامج حماية واحد و هذا طبيعي ممكن يكون اكتشفه بطريقة غلط لأن كثير برامج نظيفة كثير من برامج الحماية يعتبرها ضارة

**الملخص**

فيه طرق كثير ممكن نتخطى حمايات و نخلي محلل المالوير يتعب بس هل هذي الطرق الوحيدة؟ و هل هذا يعني ان محد ممكن يحلل او يكشف المالوير حقك؟ الاجابة لا الموضوع فقط اشبه بلعبة الفار و القط