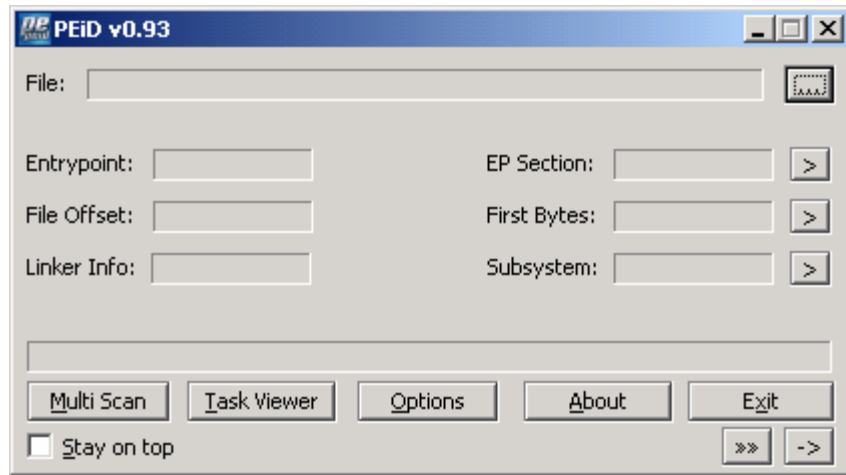


بسم الله الرحمن الرحيم

شرح بسيط لبرنامج PEiD

برنامج يعطي معلومات عن الملفات التنفيذية

صمم أصلا من طرف Qwerton من أحد البلدان المستقلة عن الاتحاد السوفيتي سابقا بلغة التجميع أو ما يسمى win32Asm ثم ساعده Snaker شاب آخر من الهند الذي قام فيما بعد بإعادة كتابته كله بلغة Visual c++ ثم التحق به المخضرم Jibz المعروف بمكتبة خوارزمية الضغط ApLib، المهم آخر إصدار كان بداية الشهر الأول من سنة 2005



يحتوي البرنامج قاعدة بيانات بأسماء برامج الضغط و التشفير و الحماية للملفات التنفيذية بالإضافة إلى لغات البرمجة المختلفة

يقوم بفحص الملف المختار و البحث عن إمكانية وجود Signature لأحد البرامج المعروفة الموجودة بقاعدته الداخلية أو القاعدة الخارجية الموجودة في الملف النصي userdb.txt

أي عندما نفتح ملف تنفيذي .exe. بهذا البرنامج يمكن معرفة:

إن كان محمي: اسم و إصدار برنامج الحماية المستعمل و مؤلفه

إن كان مضغوط: اسم وإصدار برنامج الضغط و مؤلفه

أو لغة البرمجة المستخدمة في بناء التطبيق

بالإضافة إلى معلومات أخرى حول بنية هذا البرنامج و سنتطرق لبعض منها

EntryPoint: نقطة دخول البرنامج أو بمعنى أصح مكان وجود أول أمر من أوامر

البرنامج بالذاكرة عند بداية تنفيذه، تسمى إختصارا EP

File Offset: موضع نقطة بداية البرنامج EP في الملف التنفيذي هذه المرة

فقد يختلف الوضع في الملف عن الوضع في الذاكرة

Linker Info: رقم إصدار برنامج الربط المستعمل في بنية البرنامج
EP Section: الجزء الموجود به EP الملف التنفيذي مقسم أجزاء Section لكل منها
اسم و خصائص، كمثال بسيط برنامج مكتوب بلغة التجميع عادة ما يكون به 3 أجزاء
بالترتيب:

text. يحتوي أوامر البرنامج او الكود التنفيذي
data. لا يحتوي على أي كود بل معطيات تستخدم في البرنامج
rsrc. يحتوي على الرسورس من أيقونات و أشكال مؤشر الفأرة و غيرها
لكن هذه ليست قاعدة، فيمن للمبرمج دمج الثلاث معا ليصبح لدينا قسم واحد فقط، كما يمكن
لإضافة أقسام أخرى، فمثلا في البرامج المكتوبة بدلفي نجد على الأقل 7 أقسام:
CODE, DATA, BSS, .idata, .tls, .rdata, .reloc, .rsrc
يمكن معرفة كل الأقسام الموجودة بالبرنامج المفتوح بالضغط على الزر يمين EP
Section

First Bytes: يعطي الحروف الأولى أو الأوامر الأولى للغة الآلة الموجودة بالبرنامج
التنفيذي و بإستخدام نظام 16 أو Hex وبالضغط على الزر المقابل نحصل عليها بلغة
التجميع أي يعمل لها **Desassembly** و هو مفيد جدا

Subsystem: معرفة نوع التطبيق، تطبيق بواجهة GUI أو بدون واجهة Console أو
.... و الزر المقابل يعطي معلومات أكثر حول بنية البرنامج التنفيذي PE Details به
معلومات مهمة.

الأزرار أسفل:

Multi Scan: لفحص جميع الملفات التنفيذية في المجلد الذي نختاره
Task Viewer: تعطي قائمة بالبرامج المنفذة Running Process و يمكن إختيار
أحدها و فحصه باستخدام الزر الأيمن للفأرة ثم **Load in pied (file)**

و الأزرار الأخرى أترككم تكتشفونها، فالبرنامج سهل جدا و لأنه حان وقت النوم
يمكن التواصل بالمنتدى لأي استفسار أو سؤال