# **IDA Pro Background**

## **Author. Ahmad AlFareed**

# **Section Reverse Engineering - Tools**

### **rETKit**

## Introduction

المعروف باسم IDA Pro المعروف باسم IDA Pro المعروف باسم IDA Pro و احد منتجات Hex-Rays وراء هذا البرنامج هو المبرمج IDA Pro المناصخ هو المبرمج IDA Guilfanov من ايام IDA DOS الـ IDA Pro جوهرها في خوارزمية IDA Guilfanov من ايام IDA Pro المدار كان يتم تطوير منطق الـ recursive descent في الهندسة العكسية في اداة IDA Pro تستخدم عدد كبير من تقنيات الارشادية لتحديد التعليمات البرمجية . بعيد عن عملية التفكيك نفسها اداة IDA تبذل مجهود كبير مش فقط من احد عمليتها تميز بين البيانات التعليمات البرمجية ولكن ايضا تحدد تقريبا كلشئ مثل الـ data types المستخدمة. وتبذل جهد لوضع تعليقات لعمليات التفكيك التي تم تفكيكها ممكن ان يضع اسماء المتغيرات واسامي الوظائف .

# **Hex-Rays' Stance on Piracy**

انت ك IDA user يجب ان تكون على دراية ببعض الحقائق. يوجد تقنيات يمكن تتبعها للقراصنة الذين قامو بقرصنة IDA وجعله مجاني بالكامل من خلال فرض القيود واحد التقنيات مضادات القرصنه هي يتم وضع علامة مانية على كل نسخة IDA من اجل وجعله مجاني بالكامل من خلال فرض القيود واحد التقنيات مضادات القرصنه هي يتم وضع علامة مانية على كل نسخة مرة اخرى الى ربطها بشكل فريد بمشتريها اذا ظهرت نسخة مسربة من IDA فان Hex-Rays لديها القدرة على تتبع تلك النسخة مرة اخرى الى المشتري الاصلي وراح يفقعوه باند قد راسو ويحطو بـ Black List للمبيعات المستقبلية. وتقنية اخرى لشبكات المحلية يتم بث حزمة UDP على بورت 23945 وتنتظر IDA اذا كان نسخ اخرى من IDA تعمل تحت نفس المفتاح الترخيص على نفس الشبكة الفوعية وتتم المقارنة . عند بدء تشغيل IDA على الفور. الـ افرعية بالروح بالدم احميه يجدع هاض شرف البرنامج.

### Obtaining IDA Pro

IDA Pro هو برنامج غير مجاني لقمة عيشهم من المبيعات من خلال بيع IDA Pro . يتوفر اصدار مجاني نعم محدود الوظائف هو يوجد بها الوظائف الاساسية لكن لا يواكب المواضيع الحديثة وانا بنظري المهندس العكسي الحقيقي لا يحتاج الا الوظائف الاساسية ليتعامل مع اي شيء الاصدارات المدفوعة هي لك لتسهل لك.

# **IDA Versions**

يوجد الاصدارات الحديثة واجهة المستخدم الرسومية (GUI) و Windows, Linux & OS X لم console versions وتستخدم الكلاثة. من وجهة At cross-platform GUI libraries لتوفير واجهة مستخدم مستقة على جميع الانظمة الاساسية الثلاثة. من وجهة نظر وظيفية يتم تقديم IDA في نسختين standard و advanced . يختلف الاصداران بشكل اساسي في عدد بنيات المعالج (processor architectures) التي يدعمان التفكيك لها. الـ standard يدعم تقريبا اكثر من 30 عائلة المعالجات في حين ان الاصدار الـ Supported Processors)

## Your IDA Installation

**Download IDA Free** 

**Download IDA Pro** 

يمكنك تنزيله على Linux . Windows & OS X لا مشكلة.

The IDA Directory Layout

cfg

الـ cfg directory يحتوي على ملفات configuration بما في ذالك basic IDA configuration هو idau.cfg هو configuration ويوجد ايضا idapython.cfg وايضا

ldc

الـ idc directory يحتوي على core files الملفات الإساسية التي تتطلبها IDC scripting language .

lds

الـ ids directory يحتوي على symbol files التي تصف محتويات الـ shared libraries التي يمكن الرجوع اليها في IDA . تحتوي ملفات IDS هذه على معلومات ملخصة تسرد كافة الـ inputs التي تم تصديرها من مكتبة معينة. تصف هذه الادخالات نوع وعدد الـ parameters التي تتطلبها الوظيفة ونوع الـ return ان وجد للوظيفة.

#### Loaders

يحتوي loaders directory على IDA extensions التي تم استخدامها اثناء عملية تحميل الملفات للتعرف على التنسيقات الملفات المعروفة وتحليلها مثل PE & ELF سنتم مناقشة Loader IDA .

**Plugins** 

الـ plugins directory تحتوى على IDA modules المصممة لتوفير سلوك اضافي.

**Procs** 

يحتوي الـ processor modules على الـ processor modules التي يدعمها الاصدار المثبت من IDA على الـ processor modules المعروضة كـ IDA توفر Assembly Language المعروضة كـ IDA المعروضة كـ User Interface المعروضة كـ User Interface

Sig

الـ sig directory يحتوي على signatures للتعليمات البرمجية الموجودة التي تستخدمها IDA في pattern-matching pattern-matching مما يوفر لك قدر operations . ومن خلال مطابقة الانماط تستطيع IDA تحديد التسلسلات التعليمات البرمجية كـ library code مما يوفر لك قدر قدر كبير من الوقت في عملية التحليل.

الـ til directory يحتوي على library information التي تستخدمها IDA لتسجيل تخطيط هياكل البيانات الخاصة بـ library information المختلفة.