## unpack csharp packer

بسم الله الرحمن الرحيم

سویت packer بسیط باستخدام csharp و الحین بشرح لکم کیف یشتغل و کیف تفکونة charp\_packer

بناخذ برنامج hello world و بسوي له pack و بعدها بنحاول نفكه

```
Mello World هذا هو البرنامج حقنا بس يطبع

Microsoft Windows [Version 10.0.19044.1766]

(c) Microsoft Corporation. All rights reserved.

C:\Users\kira2\Desktop\ppid\packer>powershell

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\kira2\Desktop\ppid\packer> .\pack.ps1 hello.exe packed.exe 6
```

الحين بس نسوي pack نحط اسم الملف حقنا و اسمه بعد مايصير pack و رقم سته الحين بشرح لكم ليه

## كيف يشتغل ال packer

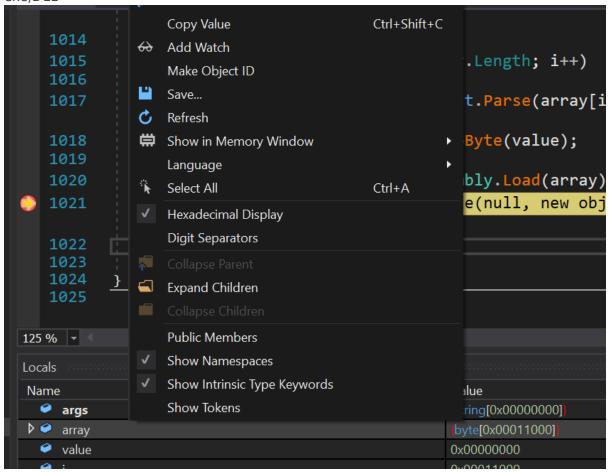
طريقة عمله هي انه ياخذ exe و يدخلة ب exe ثاني و الرقم اللي نحطه هو عدد المرات اللي يسوي الشي هذا ف بيحط exe داخل نفسه 6 مرات ليش اخترت 6؟ عشان يكون فكه ابسط كل مازاد الرقم زادت صعوبته اكثر

بياخذ exe و بيسوي له invoke و عشان اشرحه بطريقة بسيطة ياخذ بايتات exe و يشغلها في

```
memory علطول یعنی بالرام و زي مانعرف فیه 6 داخلین بعض
                   0, 0, 0, 0, 0, 0, 0, 0, 0,
                   0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                   0, 0, 0, 0, 0, 0, 0, 0, "Not showing all elements
    1006
                     because this array is too big (69632 elements)"
    1007
               };
               for (int i = 0; i < array.Length; i++)</pre>
                   int value = (int)short.Parse(array[i].ToString());
    1011
                   array[i] = Conv
                                     struct System.Int32
               Assembly assembly = Assembly.Load(array);
               assembly.EntryPoint.Invoke(null, new object[] { new string
                 [0] });
```

بحط breakpoint هنا بعدها بشغل البرنامج ) 1021 assembly.EntryPoint.Invoke(null, new object[] { new string[0] }); 1023 1025 125 % Name 🗸 🤪 array **(**0] 0x4D [1] 0x5A • 0x90 **9** [3] 0x00 **(**4] 0x03 **(**5] 0x00

لو نلاحظ في متغير array نلاقي D5A4و هي hex و تعني MZ و هذي array حقت PE مثل exe,DLL



الحين بس باخذ القيمة المخزنة في array و بحفظها ب exe ثاني

هنا بعد ما حفظناه و حطيناه ب exe نلاحظ انه نفس اللي جانا بالملف الاول بس الفرق هو البايتات تختلف بنرجع نسوي زي اللي سويناة فوق ناخذ قيمة array بكرر العملية هذي الين يطلع معنا شي مختلف

بعد تكرار العملية 6 مرات قدرنا نرجع للكود الأصلي و الحين نقدر نحلل لو كان exe داخل نفسه 100 مره كان الموضوع بيكون اصعب و ممكن نلاقي طريقة ثانية

## الملخص

كل packer بالعالم تقدر تفكة لأنه في مرحلة ما راح يفك نفسة و كثير من C# packer تقدر و كثير من c# packer على المكان اللي بيفك منه و نسحب على الطريقة اللي سويناها نحط breakpoint على المكان اللي بيفك منه و نسحب unpacking الاصلي بعد