*ذكرت في مامضى في الايام الخوالي كيف تصنع فايروس محترف لكن لم اذكر كيف تقضي عليه أو على غيره من هذه البرامج الضارة التى انتشرت حديثا في كل مكان . واني وددت اليوم أن أبيين كيف تصنع الشركات (انتي فايروس ) وكيف تقضي على الفايروسات واي فايروس ينتشر حديثا ماترى الاقليل من الوقت الا ووفرت الشركة المصنعة علاج لهذا الفايروس اللعين لانعرف كيف لكن عندما ينشتر فايروس جديد في حواسبنا تطلب منا برامج الحماية التحديث نحدثها وهيا تقضي تلقائيا على الفايروس لايهمنا كيف لكن دعونا اليوم نبيين كيف يقضون*

*عليها كيف يعالجونها ؟. اخترت اليوم فايروس اسمه ) (Soundmix بحثت عن صفاته وطريقة انتشاره ووفرت له العلاج باذن الله وما انا الابعليل قد تتسائل لماذا هذا الفايروس عن غيره ؟لان لطالما اصبح هذا الفايروس ضيف ثقيل علينا وبالاخص على مختبراتنا حيث ماتفتح قرص صلب الا وتجد فيه فولدر اسمه ( RECYCLER) اضنك الان عرفت هذا الفايروس.*

***اذن لنبد بصفاته يتميز بها هذا الفايروس :-***

*1. يخزن ملفه الاساسي ضمن ملفات النظام بهذا المسار*

*C:\WINDOWS\system32\soundmix.exe*

*لكي لايحذف من قبل برامج الحماية لانها تتجنب المسح في تلك الاماكن.*

*2.ويخزن ملفه ال ( DLL) له في*

*C:\WINDOWS\system32\dllcache\zipexr.dll*

*وشكله الخارجي الذي يظهر لنا هوا فولدر اسمه RECYCLER)) تامل ذكاء مصمم هذا الفايروس جعل نسخته الاصلية ضمن ملفات النظام ويبث على بقية الاقرص ما ان تمسحه بطريقة ما الا وتعود نسخته الاصلية ببناء النسخ المحذوفة من جديد . اذن نحتاج اولا نحذف فولدراته ومكوناتها وبنفس الوقت نحذف ملفاته الأساسية وبهذا نكون قد قضينا على الفايروس ولكثير من المعلومات عن الفايروس اكتب اسمه في اي محرك بحث وستعرف عنه الكثير .تذكر لتصمييم اي مضاد فايروس يجب ان تكون قد حللت الفايروس كاملا قبل الشروع بالعمل فالعمل بسيط لاكن التحليل يحتاج لوقت. ولا اظن الأن التحليل يحتاج لوقت فلو كتبت اسم اي فايروس في اي محرك بحث ستجد عنه كامل المعلومات:.*

**لنبدا بالعمل:سوف نبرمج ب vb.net2010 نكون فورم كما في الشكل**



*بداية نستدعي المكتبات المطلوبة في العمل*

Imports System.Collections.Generic

Imports System.ComponentModel

Imports System.Data

Imports System.Drawing

Imports System.Linq

Imports System.Text

Imports System.Windows.Forms

Imports System.Collections.ObjectModel

Imports System.IO

*الان نكتب هذا الكود في زر (بدء البحث والقضاء على الفايروس)*

نخزن جميع الاقراص الصلبة في مصفوفة'

Dim allDrives() As DriveInfo = DriveInfo.GetDrives()

نبدا بالبحث بقرص صلب تلو الاخر ضمن المصفوفة على الفايروس

Dim d As DriveInfo

For Each d In allDrives

اذا كان القرص شغال يبحث فيه

If d.IsReady = True Then

نعرف متغير من نوع قرص صلب لنسند اليه الاقراص المتوفرة

Dim di As New DirectoryInfo(d.Name)

نخزن جميع ملفات القرص الصلب المختار داخل متغير

Dim fii As FileInfo() = di.GetFiles()

نبدا بالبحث بملف تلو الاخر

For i As Integer = 0 To fii.Length – 1

**نحول خصانص الملف الى اعتيادي لان مصنعي الفايروسات يحولون خصا ئصه الى مخفي او عدم قدرة الحذف لذالك نلغي هذه الخصائص في كل ملفات القرص**

fii(i).Attributes = FileAttributes.Normal

Next

(RECYCLER )الان نبحث على الفولدر المطلوب وهو

Dim dii As DirectoryInfo() = di.GetDirectories()

For i As Integer = 0 To dii.Length - 1

If dii(i).Name = "RECYCLER" Then

عندما يجد الفولدر يحول خصائصة الى الحالة الطبيعية

dii(i).Attributes = FileAttributes.Normal

ناخد الملفات الثي بداخل مجلد الفايروس لمسحها اولا

fii = dii(i).GetFiles()

For ii As Integer = 0 To fii.Length - 1

fii(ii).Attributes = FileAttributes.Normal

fii(ii).Delete()

Next

الان نمسح مجلد الفايروس

dii(i).Delete()

End If

Next

End If

ونستمر بالعملية حتى يمسح الفايروس من جميع الاقراص

Next

الان مسحنا مجلدات الفايروس لاكن بقي النسخة الاصلية شغالة مع النضام لذالل يجب ايقافها ومسحها

نخزن جميع البرامج الشغالة الان في متغير

Dim p As System.Diagnostics.Process() = System.Diagnostics.Process.GetProcesses()

نبدا بالبحث عن الفايروس ضمن البرامج الشغالة ونوقفه عن العمل

For i As Integer = 0 To p.Length - 1

If p(i).ProcessName = "soundmix" Then

نوقف الفايروس الاصلي عن العمل

p(i).Kill()

p(i).WaitForExit()

Dim fi As New System.IO.FileInfo("C:\WINDOWS\system32\soundmix.exe")

نلغي خصائص الاخفاء وللقراءة فقط

fi.Attributes = System.IO.FileAttributes.Normal

fi.Delete()

fi = New System.IO.FileInfo("C:\WINDOWS\system32\dllcache\zipexr.dll")

fi.Attributes = System.IO.FileAttributes.Normal

fi.Delete()

نمسح النسخة الاصلية من ملفات النظام

System.IO.File.Delete("C:\WINDOWS\system32\dllcache\zipexr.dll")

System.IO.File.Delete("C:\WINDOWS\system32\soundmix.exe")

End If

Next