

.NET REVERSING PAPER #2

Tools needed:

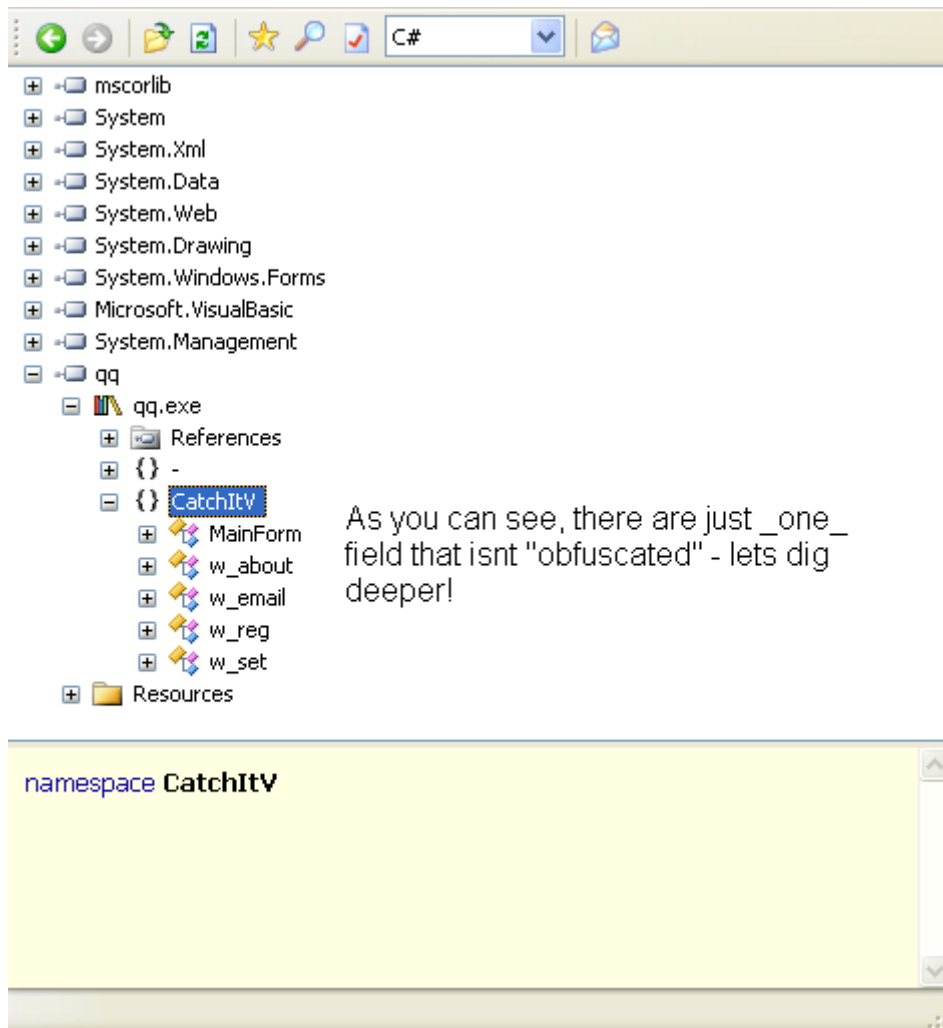
- Reflector
- MS VS 2003 or newer (Im using 2005 Team Ed.)
- RSA.NET Generator
- Brain

Tools that are included in this tutorial are; Reflector & RSA.NET Generator. Unfortunately I can't include MS VS due to the illegal stuff around it - and brain of course, that'll be your first assignment to fix yourself ;)

Now, our target today is **3D Desktop Recorder v9.0** which can be found at <http://www.dvdwindow.com/3dgame/>.

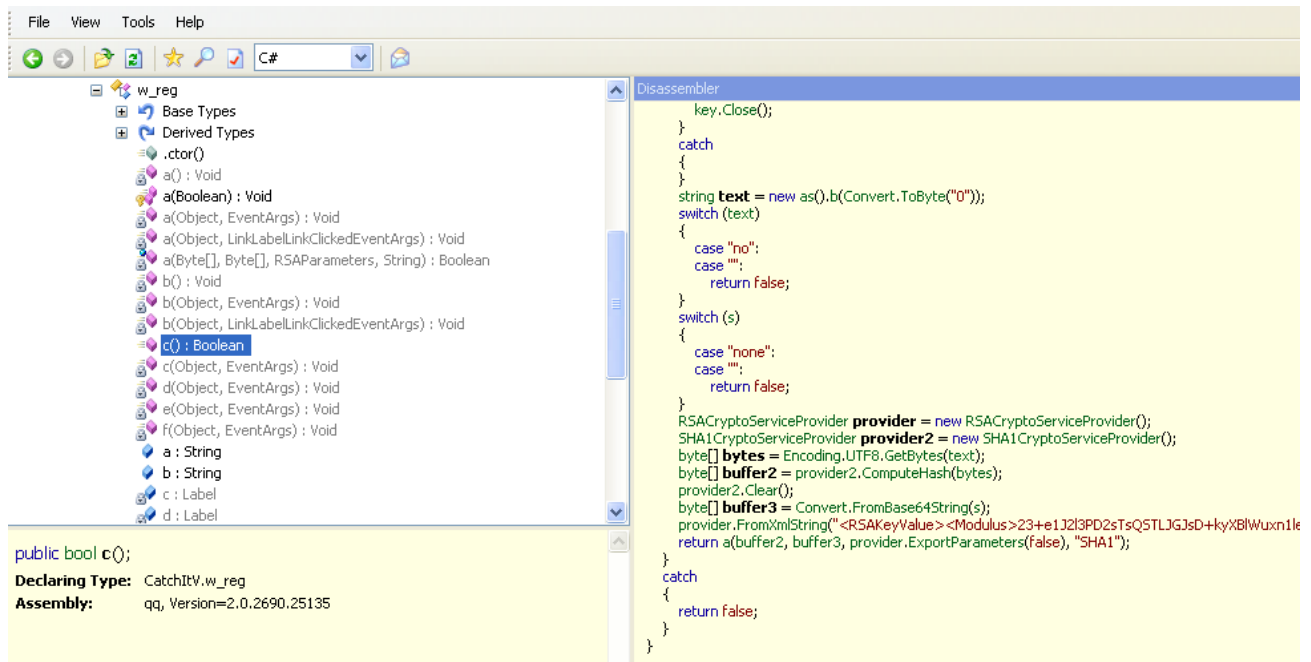
ABSTRACT

This program uses RSA-1024 as its main protection on the serial part, and our goal is today to keygen this piece. However, if you have any earlier experience with RSA - you probably know that RSA-1024 most likely cannot be factorised, so we need to patch the public key (and to those who thinks of a wiener attack, forget it - the key is too strong ☹).



Now, obfuscation shall not stop us! Hehehe, its not that hard to read between the lines ;)

ABSTRACT



And as you can see here, we have found our public RSA-key. Now, as you can also see the procedure is also shown aswell - now we just need to reverse that algorithm, and patch the current public key to one of ours ☺

Then we write our RSA code (I use C#):

```
private string RSAMe(string A_3)
{
    RSACryptoServiceProvider provider = new
    RSACryptoServiceProvider();
    SHA1CryptoServiceProvider provider2 = new
    SHA1CryptoServiceProvider();
    byte[] bytes = Encoding.UTF8.GetBytes(A_3);
    byte[] buffer2 = provider2.ComputeHash(bytes);
    provider2.Clear();
    provider.FromXmlString("<ur prvt code>");
    byte[] buffer3 = provider.Encrypt(buffer2, true);
    RSAPKCS1SignatureFormatter format = new
    RSAPKCS1SignatureFormatter();
    return
    Convert.ToBase64String(Format(buffer2,buffer3,provider.ExportParameters(true), "SHA1"));
}
```

And as you can see, I've reversed the main code here - and the rest is upto you as a cracker todo yourself ;)

Remember; im not a fuckin source-give-away-machine!

GREETZ AND HELLOS

0x87k - melatonin - lafarge - l0calh0st - c35 - ScareByte - mac...

...plus all others I've forgot :P