

Forum:[Hack Forums](#)

Thread: [Help fuding silent java drive by](#)

zanbrok - November 4, 2012, 8:54 am

I need some help fuding a silent java drive by that is posted as public on this forum as well as others. If anyone is willing to help me right now via icq, skype, msn etc. please send me a pm. Thank you .

Nieeli - November 4, 2012, 8:55 am

get proguard, I think theres a tutorial somewhere on the forum

Doku - November 4, 2012, 1:31 pm

A java drive(applet) by is never really "fully undetectable" but there are some stuff that can make decompilation harder.

As Nieeli pointed out a obfuscation will scrable around the bytecode and make decompilers have a bad time.

A few free obfuscators are: [Allatori Trial](#), [Proguard](#) and [ZKM Demo](#). Keep in mind that the main purpouse of obfuscation isnt to "protect" your code but to make your code run more efficient/faster.

An alternative would be to apply something like [classguard](#) to your applet. It basicly crypts your classes and decrypts them when being run. You can find more information about this [here](#).

Keep in that getting the decrypted classes isnt very hard at all.

You can read more about this in the article [ClassGuard UNGUARDED](#) by little0nemo.

Colby_ - November 4, 2012, 4:28 pm

(Nov 4, 2012 02:31 PM)Doku Wrote: [\[CITE\]](#) A java drive(applet) by is never really "fully undetectable" but there are some stuff that can make decompilation harder.

As Nieeli pointed out a obfuscation will scrable around the bytecode and make decompilers have a bad time.

A few free obfuscators are: [Allatori Trial](#), [Proguard](#) and [ZKM Demo](#). Keep in mind that the main purpouse of obfuscation isnt to "protect" your code but to make your code run more efficient/faster.

An alternative would be to apply something like [classguard](#) to your applet. It basicly crypts your classes and decrypts them when being run. You can find more information about this [here](#).

Keep in that getting the decrypted classes isnt very hard at all.

You can read more about this in the article [ClassGuard UNGUARDED](#) by little0nemo.fud has nothing to do with difficulty of deobfuscation..

Virux - November 4, 2012, 11:11 pm

(Nov 4, 2012 02:31 PM)Doku Wrote: [\[CITE\]](#) Keep in mind that the main purpouse of obfuscation isnt to "protect" your code but to make your code run more efficient/faster.

Adding dozens or more classes with garbage variables and functions isn't going to speed anything up. The main purpose is to make the available code demandingly troublesome to analyze.

Doku - November 5, 2012, 1:33 am

(Nov 4, 2012 05:28 PM)Colby_ Wrote: [\[CITE\]](#) fud has nothing to do with difficulty of deobfuscation.. Well, I was mainly talking about making the code harder to read for a suspicious indi individual. I

have no real experience with anti-virus detecting a drive by.

I probably should have made my post clearer. It was also not a priliant idée to post at night when being extreamly tired.

zanbrok - *November 5, 2012, 5:44 am*

thanks everyone. so since i can access the source, is there a better way to fud it other then with obfuscators?