

Re: [Full-Disclosure] Reverse Engineering thoughts

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0115.html>

From: Blue Boar (BlueBoar_at_thievco.com)

Date: 01/06/04

To: n30 <n30_lists@hotmail.com>

Date: Tue, 06 Jan 2004 11:27:38 -0800

n30 wrote:

- > *Say I am pen-testing an application...It requires authentication credentials*
- > *to run. Also, the software has a demo mode & full version mode.*
- >
- > *Now using RE (Reverse engineering), I can change the ASM & create a small*
- > *patch file to bypass the auth & convert the demo mode to full version mode.*
- >
- > *Is this a security problem?? What should be my recommendation??*

Copy protection bypass is not a security problem per se... at least, not for the user of the app. Copy protection bypass is always possible if you are willing/able to modify the binaries.

They may be interested to know how easy the bypass was (or wasn't).

- >
- > *This is assuming that I work for a pen test firm & the company wants us to*
- > *test their product. So I should not be affected by DMCA?? Am i right??*

Probably. If they've given you permission, and you've got your get out of jail free card in order. A contract giving you permission would be huge evidence in your favor.

Still, for the extraordinarily paranoid, note that Dmitry was still detained for prosecution even after Adobe dropped their complaint. Aparantly, the US Federal Government can prosecute crimes under the DMCA even without a victim.

BB

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>