{* **SOFTWARE** *}

MS Windows source code escapes onto Internet

Say it's a vital secret for long enough and it'll turn round and bite you...

Fri 13 Feb 2004 // 10:04 UTC   GOT TIPS?

John Lettice   BIO   EMAIL   SHARE

Microsoft has suffered what appears to be a severe leak of Windows source code, with a file circulating on the Internet appearing to consist of several million lines of code from around mid-2000. The source code seems to relate to NT4 and Windows 2000, and in a statement the company has conceded that "portions of the Microsoft Windows 2000 and Windows NT 4.0 source code were illegally made available on the Internet.

"It's illegal for third parties to post Microsoft source code," the statement continues somewhat redundantly, "and we take such activity very seriously."

The impact of the leak is however massively more important for Microsoft than it is for the rest of the world, as it effectively blows the company's 'security via obscurity' approach to smithereens. Over the past year or so it has, with much pomp and ceremony, unveiled its shared source programme as a counter to open source, while in the same period it has repeatedly stressed that it *cannot* disclose some aspects of its code to rivals for security reasons. If they could see it, it would leak, and then evil terrorists would be able to break into Windows more easily. Microsoft, incidentally, currently has the shared source web site as a 'related link' on the leak statement page. Are you *entirely* sure about this relationship, dahlinks?

According to Neowin, there are two packages which appear to be the source of NT 4 and Win2k, respectively. The site says it's not yet clear

whether or not the full source has leaked. Betanews says the claimed Win2k source contains 30,915 files and consists of 13.5 million lines, pointing out that this is considerably less than the 35-50 million the entire source should consist of.

This is still however a substantial slug, so if keeping source secret is important, then the leak is surely important. The leak will likely be of some help to people trying to find vulnerabilities in Windows (bear in mind that source for NT and Win2k has a great deal of relevance for XP), but the ready *illegal* availability of source presents a problem rather than an opportunity for security companies and for developers trying to make their products interoperate with Windows, given that having illegal knowledge of Windows' workings would massively compromise their ability to do legal work.

This may present particular problems owing to the likely entertainment value of Windows source. Betanews tells us that already people have been looking for the notorious "Weenies" jibe at Netscape developers, and although they've come up empty, there are numerous profanities and references to codenames long gone. *The Register* is confident that close study will reveal that it's all such a byzantine nightmare that our long-held theory that Microsoft doesn't know what's in there either will be proved, but don't look if you ever want to legally develop for Windows again.

What next? Microsoft says there has been no breach of its corporate network and internal security, which is possibly a first, but has called in the FBI. The dates of the code and the content will likely produce clues as to how and where it began to make its way out of the company, and if the mid-2000 claim is correct, that would suggest that it could have been outside of Microsoft for some considerable time. The likelihood is surely that it was associated with a development deal with an outside company whose safe has now fallen open, or something.

The weirdness here is that although Windows source code might be obscure, it's not exactly secret, nor has it ever been. Microsoft now does the shared source stuff, but it has been giving outside companies access for years. There are plenty of people out there who do know something

about Windows source code, and under shared source deals plenty people can look at Windows source, but there's not a lot of point looking if you can't do anything much with the knowledge, and if you don't have a legal, development reason to look you're not exactly going to volunteer to do so.

It'd be nice if escaping source code prompted Microsoft to take a more rational view of the whole issue, stop pretending it's secret and adopted the rival view that openness *helps* security, but we fear that'll take a few more leaks. Windows source code - so secure we let the Chinese and the Russians look. Right. ®

Tips and corrections

✉ **Sign up to our Newsletter** - Get IT in your inbox daily

➦ **SHARE**

ABOUT US   ⌄

MORE CONTENT   ⌄

SITUATION PUBLISHING   ⌄

SP SITUATION PUBLISHING

The Register - Independent news and views for the tech community. Part of Situation Publishing

SIGN UP TO OUR WEEKLY NEWSLETTER

Your Work Email Address

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

SUBSCRIBE