

Re: [Full-disclosure] Office 0day

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-06/msg00519.html>

- *From:* Valdis.Kletnieks@xxxxxx
 - *Date:* Mon, 25 Jun 2007 21:18:28 -0400
-

On Mon, 25 Jun 2007 15:46:19 PDT, phpninja said:

<i>If other places are offering \$20K for a 0day, why should Microsoft offer 10 times that, when they can probably make the sale offering only \$25K?</i>

I would think Incentive.. Sell my exploit to some criminal network for cheap? Or would I rather Microsoft trump their offer by much more and continue consulting for microsoft rather than criminal networks.

I suppose if you're bidding on a \$50 item on eBay, you bid \$500?

"No, that would be stupid, \$55 would be smart". Exactly the point.

Also if I am in any industry (lets say software) I am going to strive to produce the best product possible regardless of the profit.

Forget it. You can't get it perfect. At some point, you need to actually **ship** product. If you don't ship, you don't sell, and your company doesn't get any income. It's hard to produce a better product if all your best people just left because they haven't been paid.

It's not just restricted to the software world. Nobody seriously expects a house builder to build "the best house possible regardless of profit" – if they use \$400K of the best possible materials in the building of every \$200K house they build, they won't be in business very long at all.

Well I would think there would be some motivation. Unless every employee who codes at Microsoft is a money grubbing greedy person with no regard to the person who uses their products then there would have to be some motivation to fix the product if it is flawed.

OK. Maybe there is **some** motivation. However, most of the people who are motivated to fix it are **also** being told "the ship date for Vista has slipped

Re: [Full-disclosure] Office 0day

2 entire frikking *years*, we need to get this out the door already".

When your boss tells you "Look, I don't care how 'perfect' you can make it, I need the best version the 3 people on your team can make by July 15, or you're fired and I'll hire somebody who can deliver their code this year", most programmers will do the July 15 version, not the perfect version, because August 1 they have to make a mortgage or rent payment....

<I>Which is a better bet for Microsoft – spending \$15 million on a big PR and advertising campaign that announces the 'New Secure Attitude', or spending \$50M on quietly fixing the broken software?

</i>

lets see, they spend 50 million over 7 years (windows xp lifespan so far) not bad.. they are a 280+ billion dollar company.

These were example numbers. I'm positive they spent much more on both advertising and bugfixing. The point still remains that they're there to make a profit – and they make more profit if they do a PR song-and-dance than if they actually work on securing the software (which is a *very* hard and expensive thing to do when it's 50 to 100 *million* lines of code, with lots of inter-dependencies, and huge backward-combatibility minefields to worry about as you try to fix code).

So explain to me again why they should spend \$200M to fix it right, when they can spend much less doing PR, and people will still buy it anyhow? If there was more serious competition, then actually doing it *right* would matter. But when 90% of the people would buy Microsoft DogCrap 2007 as their next OS just because it's got the Microsoft flag logo on it, there really isn't any big reason to spend lots of time and effort on real security.

So what they want is the *cheapest overall* way to keep Joe Sixpack and Jim McCorporate from saying "I wonder if I should convert to OSX or Linux". It doesn't have to be perfect. It doesn't have to be "the best". It just needs to be *cost effective*. Consider the following (made-up) numbers.

- 1) You make \$50 per copy sold.
- 2) 10 million people are considering switching.
- 3) A \$10M and and PR campaign is enough to snow-job 8 million of them into staying, because they're sheeple and easily herded.
- 4) You could stop another 1 million from switching, but it will cost you an estimated \$100 million to do the work to fix the actual problems.

What do you do? Keep in mind that in this example, you're a publicly traded corporation in the US, and as such, have a legal responsibility to maximize the return to the shareholders.

Re: [Full-disclosure] Office 0day

Re: [Full-disclosure] Office 0day

*<i>Microsoft could *easily* argue that the webmaster or sysadmin or whatever *should* have known that "software is hackable" and taken additional precautions of their own.</i>*

That is like me trying to argue that after going to a car mechanic, I should have known that the engine mount that I paid to be secure in my car would have loosened on a bumpy freeway and let my engine fall out on the freeway.

No. Wrong analogy.

The right one would be the car dealership trying to argue that the car was built right, and was working perfectly when they sold it to you, and that you should have *known* that cars require a certain level of routine maintenance, and it isn't *their* fault that you didn't either check the engine yourself or pay somebody to do it when that "oil pressure" light came on....

Or maybe a better one – you go to a mechanic to get new high-bling tires and rims installed, and 200 miles later one falls off because the nuts loosened. You'll have a hard time winning that lawsuit against the mechanic if your car's owners manual recommends that after changing tires, you re-check the lug nuts after 40 or 50 miles, to make sure they've stayed tight.

I should have put a big metal sheet under my car from keeping things from falling out after i pay for service!! I just should have that knowledge magically. It just won't hold up in court.

No, it isn't "magically" – there's a legal concept called "due diligence". It means that you're responsible for making sure that the research gets done. If you're a car owner, it means you need to follow the suggested maintenance and change the oil as needed, and drive obeying the local laws. If you're buying a house, it means you get an inspector to check for structural defects, and a lawyer to do a title search. If you're starting a day care center, it means you do at least *some* research to make sure you're not building on a known toxic waste dump or similar hazard.

And if you're starting an Internet-based company, it means doing your research and finding out that you need to pay for hosting, and bandwidth, and that sites get hacked, and how much it costs for hosting and bandwidth and getting your site de-hacked, and so on.

*<i>Making a *criminal* negligence case stick would be *exceedingly* hard to do</i>*

I don't think it would be so hard. Someone reports a critical flaw, and microsoft reports it, but doesn't patch it and does nothing about it. So they know about the flaw at hand and aren't doing anything to fix it. That

Re: [Full-disclosure] Office 0day

Re: [Full-disclosure] Office 0day

is the definition of negligence.

Answers.com says "(law) recklessly acting without reasonable caution and putting another person at risk of injury or death (or failing to do something with the same consequences)" (<http://www.answers.com/topic/criminal-negligence-culpable-negligence>)

There really **is** a "you're going to get somebody killed doing that" component to criminal negligence.

And "aren't doing anything to fix it" isn't an easy sell for the DA either. I can just see the defense attorney at closing arguments:

"Members of the jury, by keeping quiet about the bug and not shipping a patch, the software vendor was actually protecting the user community. Yes, several hundred or maybe a few thousand machines had been compromised by way of this bug – but experience has shown us that once a patch becomes available to the general public, it leads to the release of viruses and worms that target the literally millions of machines that haven't been patched yet. Past experience has shown that the best way to minimize the number of machines attacked is by keeping it secret, and slipping a fix into the next 'service pack' where it won't be noticed among all the non-critical fixes..."

(Think about it – how many worms have we seen that incorporated a 0-day? How many boxes get pwned by a **true** 0-day that's not widely known, how many get pwned between when the bug becomes generally known and when the patch comes out, and how many get pwned after the patch comes out?)

Think you stand a chance of convincing **everybody** on the jury for a criminal conviction?

Its like a tire company knowing of a problem in their tires, stating the problem, and not recalling the tires.

It's just a **little** bit different when people are getting killed when the tires fail.

They know of the problem but don't fix it. Now I've been thinking, I dont think you'd need a big DA or anything of that nature.

You're going to need a DA who's big enough to be able to convince the people who pay him that he should be chasing this lawsuit against Microsoft, and that it's more important than the murderers and drug dealers and all the other criminal cases already in the system. Especially when you know that it's going to be a long and expensive trial and will tie up a courtroom for months.

If you're approaching it as a civil case, you will need to find an attorney

Re: [Full-disclosure] Office 0day

Re: [Full-disclosure] Office Oday

that's either willing to do it pro bono (i.e. without planning to get paid for the next 2 or 3 years worth of work), or a case where the damages caused by the alleged negligent behavior are high enough that their 30% of a judgment would make it worth their time, or bill at \$200 per hour for a *lot* of hours....

There was a judge in the news recently suing for \$60,000,000 for a pair of pants. All you have to do is piss off the right people.

Said judge got told where he can stick his lawsuit. It was ruled today in favor of the dry cleaners. <http://www.msnbc.msn.com/id/19414287/>

Attachment: [pgpIAkNfS1Iyb.pgp](#)

Description: PGP signature

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>