A Step Towards Information Anarchy: A Call To Arms

By hellNbak

Recently, Scott Culp of Microsoft's Security Response Team released the following paper:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp

Since the suspiciously timed release of this paper, rumors are that Microsoft has been contacting the management of various research groups to discuss with them their disclosure policies and how to fall into the new Microsoft line of thinking. Unfortunately, I have not been privy to any of these discussions with Microsoft, but one can only guess that their intentions are not pure. I am not going to write another rant on why I think Microsoft is out to lunch and how I know for a fact that they would like to force legitimate security research into the grave and return to the days of not spending money on security, but I am going to write a rant on what I think the research community needs to do to help Microsoft and all vendors see the light. Make no mistake about it - Full Disclosure is in clear and present danger of being stomped out by vendors like Microsoft.

Back in the day, groups like ADM, Rhino9, L0pht, and w00w00 would responsibly release advisories with complete details and proof-of-concept code. Security was improving, vendors continued to get the message that their software had better be secure, and that they would be forced to deal with serious security issues. Or did they? Unfortunately, it seems the only message that the software vendors learned was that security issues are expensive, and while money should be spent convincing the public that the vendors care about security issues, the full disclosure community needs to be crushed so that things can go back to business as usual. To Microsoft and vendors like them, security is not a technical or a developmental issue; it is merely a marketing issue that can be -

and is - leveraged for press time.

Unfortunately, today, Rhino9 is no longer and ADM has been quite quiet - keeping things to themselves no doubt. L0pht is now a consulting organization and w00w00 has also been very, very quiet. To add to the problems, we have groups and people like Georgi Guninski, who while releasing some very interesting research and proof-of-concept code, refuse to do it in a responsible manner, giving the vendors all the ammunition they need to attack the full disclosure community.

So how do we fix what seems to be broken beyond repair? How do we take the power away from the software vendors and return it to the research community? My answer is: INFORMATION ANARCHY. Microsoft likened researchers - not criminal hackers or script kiddies - to terrorists holding software companies at ransom and being irresponsible by releasing proof-of-concept code. Microsoft claims that we are in a state of "Information Anarchy" and that the research community must be stopped. Do we really want to return to the olden days when vendors knew they could ignore security issues? I say no; it has to stop and the only way to stop it is to demonstrate to Microsoft and the world what _true_ Information Anarchy is. I propose that everyone who is involved in security research and supports full disclosure steps up research efforts and releases those issues that they have been sitting on. Let's flood the security department of every vendor with new issues. Let's show the world what they would miss and what information could just as easily have stayed in the underground rather than be posted to Bugtraq or Vulnwatch.

Before you go out and start releasing all your zero-days, I do caution this with the recommendation that we all put in the effort to coordinate with vendors before releasing the advisories. I do not mean you should sit on something for 90 days until the vendor decides to fix it, but I do think that the vendor should be notified and given a set amount of time (30 days to fix and 5 to respond, perhaps) to respond properly. While we need to be direct with our actions, we do need to exercise caution and responsibility.

Show your support for this movement; help us take the power back from the vendors. I am offering my free time to help anyone with a security issue

to report it to the vendor and craft an advisory. I am also asking everyone in the research community who supports full disclosure to release advisories in support of what I am calling Information Anarchy 2K01.

We have had the lame, media-created defacement wars between script kiddies - now it is time to wage a true war that will demonstrate our skills, and more importantly, demonstrate to the vendors, the corporations, and the world, what they are forcing into the underground.

I am not asking anyone to do anything illegal, I do not want to see any supportive defacements or hacks but I do want to see some supportive advisories and research efforts. Microsoft just spent the last few years fighting for their "freedom to innovate" and now they are trying to take ours.

For information, help, or comments please email hellnbak@nmrc.org.