

BPM and SOA

Free Independent Review of BEA's BPM Suite and ROI

www.bea.com/soa

[Ads by Google](#) - [Advertise on this site](#)



Q&A: Why Metasploit Publishes Hacker Tools

H.D. Moore, head researcher of hacker organization Metasploit, talks about why it's important to publish security exploits, the organization's relationship to the cops, and more.

By Larry Greenemeier, [InformationWeek](#)

Oct. 23, 2006

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=193400966>

The [Metasploit Project](#) takes penetration testing to a whole new level, not only finding vulnerabilities in applications, but also providing exploit code that so-called white hat and black hat hackers alike can use to test the real-world implications of these vulnerabilities. Metasploit founder, developer, and researcher [H.D. Moore](#) took some time away from his work on the [open source Metasploit tool](#) and his day job as [BreakingPoint Systems'](#) director of security research to talk to *InformationWeek*.

InformationWeek: What is the value in publishing an exploit?

H.D. Moore: Exploit code allows network administrators, security software developers ([HIPS](#), [IDS](#), [IPS](#)), and penetration testers to actually verify and investigate a vulnerability. Without exploit code, penetration testers can't do their jobs, IDS developers can't create reliable signatures, and network administrators have to blindly trust that a patch installation actually worked.

IW: What is Metasploit's policy for publishing exploit code? Do you give a vendor a certain amount of time to respond?

Moore: The author of each individual exploit module is responsible for deciding when their code should be released. The Metasploit staff does not enforce anyone's idea of "responsible disclosure" and each of us have our own policies for when to release an exploit based on the patch timeline. I typically wait for a patch to be released, but make exceptions when the vendor is particularly slow to resolve an issue.

IW: Have you ever been confronted by vendors or law enforcement asking you to stop producing exploit code?

Moore: No vendor has been brazen enough to actually ask yet. I have talked to a few folks that work in law enforcement that are actually huge fans of the project.

IW: What was the reaction, both from browser vendors and programmers, to your July campaign to expose different browser bugs all month?

Moore: [Mozilla](#) responded quickly to all issues and went so far as to proactively test certain areas of their code, using

tools we developed. They even sent me a T-shirt. Apple never responded to the [Safari](#) bugs we published, but finally released a patch for the code execution flaw last month. [Opera](#) resolved each issue we posted in their weekly builds and eventually integrated all of these fixes into their next stable release. Microsoft was quick to respond early on, but then stopped sending progress updates. It wasn't until a working exploit for the [setSlice\(\) vulnerability](#) was posted that they bothered to give me a status update on the other 90+ pending issues.

IW: Is Metasploit funded entirely through donations?

Moore: I pay for most of our expenses out of pocket, but external donations have helped cover things like hosting, artwork, and conference attendance. A few months ago, we created a LLC and transferred all copyrights, trademarks, and domains to this company. The three members of the LLC are Matt Miller (also known as Skape), Spoonm (who prefers to be known only by his handle), and myself. This company exists for the sole purpose of holding the intellectual property of Metasploit and helping us enforce copyright and licensing violations. We have no commercial plans.

IW: What's the largest single donation Metasploit has received?

Moore: The largest single external contribution we received was \$500.

IW: What is Metasploit's relationship with the Hacker Foundation?

Moore: [The Hacker Foundation](#) manages the Metasploit Fund, which all new Metasploit donations filter into. Matt Miller, myself, and one of the Hacker Foundation board members manage this fund. This fund is used to promote security research and expand the functionality and features of the Metasploit Framework.

IW: How many exploits and payloads are currently available on Metasploit?

Moore: The most recent numbers are 156 exploits and 76 payloads. An exploit triggers the bug and injects the payload, which is whatever happens after the code is injected.

IW: Why is Metasploit developing a GUI interface for its framework?

Moore: We're starting to give in. At first, we wanted the Metasploit framework to be a tactical tool, used only by people who know what they're doing. But 90% of our users are using the Windows version, even though Metasploit was written as a Unix platform. Metasploit doesn't work as well on Windows, and we want to improve that. This will cut down on the support e-mails we get.

IW: What does it feel like to speak before packed audiences at shows such as [Black Hat](#) and [Defcon](#)? Do you feel this validates your work?

Moore: It's exciting to see that so many people are interested in the research and software that I work on. The community that has sprung up around the Metasploit Project validates my work more than anything. It's great to see people using the Metasploit Framework as a research and development platform and not just an easy way to launch exploit code.

Return to the story:

[Is The Metasploit Hacking Tool Too Good?](#)

TAKE OUR POLL

Metasploit: Help Or Menace? : Metasploit publishes tools to automate developing exploits that take advantage of security holes in software products. Is that right?

Call center phone system - benefits of IP & multimedia

Replay our Dec webinar - free www.team-sos.com/contactprofits

[Ads by Google](#)

[Advertise on this site](#)

Copyright © 2006 [CMP Media LLC](#)