

Data Virtualization & SOA

The Role of Data in SOA Free Forrester Report www.bea.com/soa

[Ads by Google](#)

[Advertise on this site](#)



Is The Metasploit Hacking Tool Too Good?

The open source project already offers penetration testing tools and exploit code. Now it's going further, offering eVade-o-Matic, a tool to make it harder to detect exploit code aimed at Web browsers. Has the group gone too far?

By Larry Greenemeier, [InformationWeek](#)

Oct. 23, 2006

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=193401125>

Has H.D. Moore gone too far?

Moore's like many security researchers who gin up publicity for the software flaws they find, as he did with his bug-a-day stunt highlighting browser weaknesses in July. But he goes further, as one of the main forces behind the Metasploit Project, which posts a free, open source platform that makes it easier to develop and test code that can take advantage of software vulnerabilities. Included are more than 150 examples of such code ready to exploit flaws.



Don't cry to Moore

Next month, Moore will raise the already-high stakes when Metasploit releases a new piece of code--called eVade-o-Matic--that makes it harder for intrusion-detection systems and antivirus software to detect exploit code aimed at Web browsers. It's one thing to show people how to exploit software flaws; it's another to help attackers go unnoticed.

The Metasploit Web site serves as a mental gymnasium for security pros--and cons, since it makes no effort to discern one from the other--looking for ways to break into IT systems. The latest effort, eVade-o-Matic, is designed to disguise malicious JavaScript that's used to attack browsers; it takes normal JavaScript that programmers write into a Web page and makes it look different each time the page is launched. That can foil software defenses that rely on lists of known malware.

Metasploit's self-proclaimed quest is to help IT pros verify the security of the software they buy or write. "Without exploit code, penetration testers can't do their jobs, [intrusion-detection system] developers can't create reliable signatures, and network administrators have to blindly trust that a patch installation actually worked," says Moore, a developer and researcher for the site he helped launch in 2003. Moore's work amounts to that of an arms dealer or gun maker: His wares can be used to protect or endanger people. He's not interested in controlling how his goods are used.

Moore and his Metasploit colleagues are used to blurring the line between improving security and creating insecurity. Moore last month created an exploit of the now-patched Vector Markup Language, or VML, vulnerability in Internet Explorer. That exploit was undetected by 26 virus-scanning engines, including those from Kaspersky, McAfee,

Microsoft, and Symantec. Earlier this year, Moore created a zero-day exploit--one unleashed before there's a known remedy--to take advantage of a vulnerability in Microsoft's Windows Metafile. That prompted Microsoft to take the rare step of releasing a patch five days ahead of its software-patch schedule. Moore added to his prestige and forced Microsoft to fix its problem sooner, but he also left Internet Explorer more vulnerable than if he'd worked discreetly with Microsoft.

'As White Hat As You Get'

Moore's a celebrity in the security community. His presentation at the Black Hat Conference in Las Vegas this summer was packed as he discussed the latest version of Metasploit vulnerability-testing software. There are two ways to look at Moore and his ilk: They give malicious hackers better ability to attack customers of Microsoft and other popular products; or they show tough love to software companies so they'll produce more-secure products.

In security circles, Moore's viewed as straight-laced--"probably as white [hat] as you can get," says Mati Aharoni, lead penetration tester with Israeli company See Security Technologies. A clean-cut 25-year-old native of Honolulu, Moore hardly looks the rogue of Metasploit.com, with its image of a sneering programmer staring at a screen through a black mask.

He's even well regarded by some--not all--in Microsoft's Security Technology Unit, which had Moore speak at its "Blue Hat" conferences, designed to give Microsoft programmers a wake-up call to the kind of hacking their work will endure. However, one manager of a product successfully broken with his tools, who's no longer with Microsoft, called Moore the "spawn of the devil" and "Hitler's driver."

There's definitely some smiling through gritted teeth when Metasploit comes knocking. An open source community, Metasploit is governed by Moore and researcher Matt Miller, aka "Skape," with exploit code contributed by programmers from around the world. "The Metasploit staff doesn't 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 time line," Moore says.

This summer, Moore placed the browser community in his crosshairs, dubbing July as his "month of browser bugs" and promising to publish a new exploit for a major browser every day. Moore estimates he discovered 80 to 120 flaws in browsers during the month. Mozilla responded quickly and tested certain areas of its code, using tools Metasploit developed. "They even sent me a T-shirt," Moore says. Opera also responded weekly.

No T-shirt from Apple, though. It didn't respond to Safari bugs Metasploit published, though the company in September patched one problem Moore flagged.

Not The Only Rogue In Town

Plenty of penetration-testing tools similar to Metasploit are for sale, complete with lots of exploit code, from companies like Argeniss, Core Security, Gleg, Immunity, and Saint. There are hardware-based testing boxes from companies such as Moore's employer, BreakingPoint Systems. However, as an open source project, Metasploit is more controversial because it's more widely accessible. The same can be said for milw0rm.com, another site that provides free exploit code downloads. "Similar professional exploitation tools, such as Core Impact and Canvas, already existed for wealthy users on all sides of the ethical spectrum," writes the hacker Fyodor, in ranking vulnerability tools on his Web site, Insecure.org. "Metasploit simply brought this capability to the masses."

A Hacker Site's Highlight Reel

2003

Metasploit founded, giving exploit code to the masses

2004

Metasploit 2.0's graphic interface makes it easier to use

2006

Metasploit becomes a limited liability company, protects intellectual property from commercial use

Version 3 of the Metasploit due, with Windows interface to make it easier yet to use

Since Metasploit is open source, it's hard to tell how many people use it. Moore gets a rough estimate--90,000 this year--by tracking the unique IP addresses of people who've downloaded the latest version. Moore hopes by year's end to deliver Metasploit version 3, written using Ruby rather than the Perl programming language. It's a more robust version that promises an easier-to-use interface, something in demand given that 90% of Metasploit's users run it on Windows.

Making the product easier to use makes it accessible to more people, good or bad. Moore's not tied in knots about that. "Admins cry, 'You can break into my systems now,' " he says. "Well, you should patch your systems."

-- *With Gregg Keizer*

Continue to the sidebar:

[Q&A: Why Metasploit Publishes Hacker Tools](#)

Secrets of call center - technology on demand webcast
Hear real world rollouts, ROI www.team-sos.com/contactprofits

[Ads by Google](#)

[Advertise on this site](#)

Copyright © 2006 [CMP Media LLC](#)

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?](#)