

Topic:  Security

Fun With Hackers: Mykonos WIPS Plays Tricks to Prevent Attacks

added by [Karen Hanna](#) on January 30, 2012

1	1	Share	Share
---	---	-----------------------	-----------------------

Mykonos, a San Francisco based web intrusion prevention systems (WIPS) start-up, raised \$4M in early stage venture funding for a security system that uses deception to potentially "hack the hacker." Instead of merely blocking access, the system gives the hacker a false way in and then wastes his time, making hacking a more time-consuming, costly, and frustrating game. According to an article in [Technology Review](#), the company targets hackers who use automated tools to gain access to Web sites, essentially exploiting the vulnerabilities of the tools to first identify an attack and then waste the attacker's time with false information.

Mykonos' approach, on the surface, seems to run counter to traditional methods used by most IT departments at small and midsize businesses (SMBs)--methods that include proactively identifying security holes in the infrastructure and then plugging the holes, looking for known attack signatures, and running network security software to detect intrusions. But it offers an intriguing take on the problem of keeping up with the ever-changing cyber attacker, one that seems to address the most common hacker and the most likely hack scenario that an SMB will see.

A late 2011 survey by [Red Seal Networks](#) and Dimensional Research found that more than 75 percent of IT professionals surveyed believe that hackers with automated tools may have an advantage in getting by common enterprise security controls. It is believed that because these common measures are used with frequency across many industries, the automated tools that hackers use have gotten better at overcoming them, to the point that IT security pros are just trying to keep up. Enterprise IT also may lack the metrics needed to effectively monitor everything under their scrutiny. It stands to reason then, that novel approaches such as the use of deception might lead to improved security.

Mykonos' software takes the approach that most hackers use automated tools for a quick and cheap attack, and so the software sets out a trap to catch the cyber attacker. The trap consists of bits of code placed in the most likely places for manipulation by an automated attack tool, such as in Web pages or forms. Once an attack is confirmed, the system then engages the attacker with fake information and false paths to follow, giving him the illusion that the hack is successful. The system ultimately tags the attacking computer with a supercookie or otherwise identifies it so that future attempts to break in will be detected.

While some security experts don't believe that this approach is the best, citing possible retribution when the trick is discovered, the notion that it is possible to interject detection points into a system to discover an attack before it occurs is likely to change the future game of web intrusion detection. For now, it may thwart the progress of the most annoying hackers, at least for a little while.



About the Author



Karen Hanna
Member since June 2011

Retired engineer with over twenty-five years experience in artificial intelligence applications development for both commercial and government clients. Former Assistant VP for a Fortune 500 company.

[Full description »](#)

Related

[European Union Proposes Reform of Data Protection Rules](#)

added by [Launie Sorrels](#) on February 2, 2012

1 1

[Carrier IQ: How Big Brother Got in Your Phone](#)

added by [Launie Sorrels](#) on February 2, 2012

1 0

[Symantec Suspected of Scaring Users Into Buying Full Versions](#)

added by [Brandy Courtade](#) on February 2, 2012

1 0