

Subscribe



Sign up now and get the best business technology insights direct to your inbox.

- Daily Edge
- Business Tools & Templates
- Aligning IT & Business Goals
- Maximizing IT Investments
- IT Careers

Enter E-mail Address

SUBSCRIBE

Most Popular Posts

- [A General Lack of Compliance Cooperation](#)
- [RSA Sees GRC Moving to the Cloud](#)
- [Building a Social Business](#)
- [File Transfers via the Cloud Create a Security Issue](#)
- [Centralizing Governance, Risk Management and Compliance](#)

Recent Posts

- [Using IT to Transform the Legal System](#)
- [Managing a Social Business](#)
- [Making Big Data Really Accessible](#)
- [File Transfers via the Cloud Create a Security Issue](#)
- [Dell Tackles Microsoft SharePoint Management Issues](#)
- [IT Security Goes Virtual](#)
- [Network Monitoring Becomes a Business-Critical Issue](#)
- [Cyber Liability Insurance Becoming a 2012 IT Health Care Priority](#)
- [Pushing the Limitations of Distributed Computing in the Cloud](#)
- [Microsoft Finally Delivers on Information-at-Fingertips Promise](#)

By date:

- [January 2012](#)
- [December 2011](#)
- [November 2011](#)
- [October 2011](#)
- [September 2011](#)
- [August 2011](#)
- [July 2011](#)
- [June 2011](#)
- [May 2011](#)
- [April 2011](#)
- [March 2011](#)
- [February 2011](#)
- [January 2011](#)
- [December 2010](#)
- [November 2010](#)
- [October 2010](#)
- [September 2010](#)
- [August 2010](#)

Time to Stop Turning the Other IT Security Cheek

Posted by [Michael Vizard](#) Dec 28, 2011 1:30:18 PM

They say the best defense is a good offense. When it comes to IT security, however, IT organizations can only take the good offense so far before they wind up breaking the law themselves. But that doesn't mean they need to idly stand by and suck up attack after attack. Instead, they can disrupt the attacks on their IT systems in a way that eliminates the economic incentive for launching those attacks in the first place.

To give IT organizations the tools they need to disrupt attacks, **Mykonos Software** created a security appliance that detects when scripts used by botnets are accessing files on a site. It also detects overwhelmed scanners that hackers use to identify vulnerabilities with fake data, keeping track of the devices that were used to generate those attacks. It even gives attackers access to passwords that provide them with reams of fake data that they would need to manually sort through to find anything useful.



According to David Koretz, president and CEO of Mykonos Software, the basic idea is to use deception to make it impossible for hackers to leverage automation in any meaningful way. Once that is accomplished, it's no longer economically attractive to manually hack a website looking for a vulnerability to exploit. Now Mykonos is extending the scope of its security approach to **include applications running on the Amazon cloud service.**

What Mykonos is doing, says Koretz, is overwhelming hackers who are using any number of automated tools with a sea of garbage data. Sorting through all that data becomes too time-consuming for the hackers, who wind up not being able to make as much money because they have to rely on manual processes to discover vulnerabilities. As a result, Koretz says the profit motive for hacking a particular site or application is sharply reduced. Koretz maintains that this deceptive approach is far more effective than relying on antivirus and firewall technologies that are built around castle-and-moat approaches to security that can't respond to threats in an age when there is no such thing as an enterprise perimeter.

While leveraging the information gathered by Mykonos theoretically makes it possible to go on the offensive, Koretz cautions customers not to take the law into their own hands. That's especially important, adds Koretz, at a time when it's **not clear what attacks are being sponsored by nation states** that could easily create a situation where an IT organization could find itself suddenly creating an international incident.