

Follow Us



SMARTER STRATEGIES

Honeypot Code Hacks Back at Hackers

R. Colin Johnson | Date: 02-22-11 | 1 Comment

 |  Print  PDF | Filed Under: Smarter Strategies

A former National Security Agency cyber-security chief claims proactive responses are needed to prevent cyber-threats from materializing. The proposal: Use honeypot code to identify hackers in real time and hack them back.

Former National Security Agency cyber-security chief Prescott Winter recommended to the Internet Industry Association recently that IT needs to take the initiative in protecting online businesses from the cyber-crime currently sweeping the globe.

According to Winter, current security tools use very few active countermeasures to hack back at hackers, for fear of misidentifying a legitimate user as a hacker—usually called a "false positive." As a result, most security flaws are only identified and patched after a successful intrusion has taken place. Security suites do sometimes scan for suspicious signatures or behaviors, but the number of false positives per true hacker detected can be as high as 100-to-1, according to security specialists [Mykonos Software](#) (Burlingame, Calif.).

To mitigate the false-positive problem and enable active countermeasures to target hackers, security companies are pioneering the "honeypot" approach.

"False positives are a real problem," said Wendy Nather, senior analyst at The 451 Group (New York). "Inserting what I call 'honey code' into the application stream is a very intriguing approach."

According to Mykonos CEO David Koretz, traditional firewalls are flawed, in that the protection they provide is based on patches that plug vulnerabilities only after they have been discovered.

What is needed instead is a security suite that prevents attacks by setting up software tripwires that identify hackers by recording their exploitation of known security flaws. That's where "honey code" comes in, trapping hackers by inserting known flaws into applications—flaws that hackers mistake for vulnerabilities. Once this honey code snares the hackers, they are cordoned off and led through a series of faux-vulnerabilities that test their sophistication progressively.

SEARCH

Click here for "THINK" Leadership Forum Presentation Videos

IBM RESOURCES

- End to End Virtualization: A holistic approach for a dynamic environment.
- Business Analytics and Optimization Jumpstart: Embedding analytics to transform insights into action
- Cloud computing insights from 110 implementation projects
- Capturing the Potential of Cloud
- Analytics - the new path to value
- Social Business: Advent of a new age
- Becoming a Social Business: The IBM Story

MOST READ

TRENDING

RELATED CONTENT

ADVERTISEMENT

VIDEOS



Security Monitor Dashboard tracks intrusion incidents, identifying hackers by assigned handles, determining the risk each presents by the complexity of each attack, as well as profiling by session and time period.

"We intentionally inject vulnerabilities into applications, allowing our tripwires to identify hackers in real time with 100 percent reliability," said Koretz.

Mykonos' security appliance product—a firewall that is available as software or on optimized hardware—provides IT managers with a Web-based dashboard that tracks intrusion incidents, calculates the risk each hacker presents and then monitors their network sessions.

IT can use the information to set up a variety of proactive responses to hackers, from storing secret cookie-like identifiers on the hackers' own computers to putting up a screen on the hackers' display that shows their location on a Google map.

Taking the fight directly to the hackers may represent a powerful new way to combat cyber-crime.



TWITTER FEED

IBM about 3 hours ago For those who joined the Dec. #cloudchat -- panelist @angelluisdiaz has a new post up on @Wired on SLAs in the cloud http://t.co/fvPmgM7

IBM about 3 hours ago RT @angelluisdiaz: Check out my latest blog about the importance of SLAs in the #Cloud @wired http://t.co/fXb9OTcZ #ibmcloud #cloud #clo ...

IBM about 3 hours ago Answer our question of the week: What are the top items you want in the open source #cloud? Comment here: bit.ly/sVa3Md

IBM about 22 hours ago In case you missed it: Is ITSM (as we know it) over ...

< Prev Next >

JOIN US

f Like us on Facebook

t Follow us on Twitter

Get the Smarter Tech Newsletter