



3 October 2008

Infoblox builds DNS firewall

Bryan Betts

IP network services appliance vendor Infoblox has added a new type of security feature to its hardware's NIOS operating system. It said that the upgrade would allow its DNS and DHCP devices, which cost from \$2500, to work as a kind of DNS firewall.

The updates are intended to counter attacks based on DNS exploits - such as the recently revealed DNS cache-poisoning vulnerability - by adding monitoring and reporting capabilities, so network admins will get an alert if the system is attacked. They also allow the Infoblox devices to mitigate DNS attacks, for example by throttling back connections from a specific server.

"Everything breaks when DNS breaks," said Dan Kaminski, the researcher who discovered the cache-poisoning vulnerability, which could let an attacker divert Internet traffic to malicious sites without detection.

"So now the DNS vendor needs the ability to patch easily and detect attacks," added Karl Driesen, Infoblox's EMEA vice-president. "We think it's better to fix the problem at the DNS server, rather than leave DNS weak and try to stop attacks with an IDS, say."

Driesen said that while that specific vulnerability has been patched, it had focused attention on DNS as a potential target for crackers and criminals. He said that enterprises could either deploy the Infoblox appliances as their sole DNS/DHCP service, or install them as a protective outer layer, acting as a DNS firewall to protect weaker internal Windows or BIND servers. In the latter case, the Infoblox devices would operate in DNS forwarding mode and handle recursive DNS queries, while the internal servers would handle non-recursive queries.

Branko Miskov, the product management director of rival IP address management developer Bluecat Networks, claimed that Infoblox was largely just playing catch-up. He said that other DNS specialists already treated recursive and non-recursive queries separately. However, he welcomed the connection-throttling capability as a useful addition.

The updated DNS software is free to Infoblox customers on maintenance, Driesen said.