



Press Release

Media Contact:

Atchison Frazer
Fortinet, Inc.
+1 408 235 7700 x318
afrazer@fortinet.com

Fortinet Alerts Customers to Use Multiple Defenses in FortiGate™ Systems to Defeat 2nd Phase of SoBig.F Worm Attack

SANTA CLARA, Calif., Aug 22, 2003 — Fortinet – the only provider of ASIC-powered, network-based antivirus firewall systems for real-time network protection – is alerting customers to use the port-blocking capabilities in their FortiGate™ Antivirus Firewall systems to protect against the second phase of the W.32/SoBig.F virus attack.

Fortinet started protecting customers from the most recent SoBig variant via an update delivered automatically to FortiGate units on August 19. All registered FortiGate customers whose systems are configured to accept automatic “push” updates receive antivirus signature database updates for this attack and others within minutes of Fortinet’s release of a new attack database by the Fortinet Threat Response Team.

Virus researchers have determined that the systems infected by the SoBig.F worm will attempt to contact a number of servers distributed across the Internet and will attempt to download additional malicious code. In order to prevent this, Fortinet has issued a FortiResponse Alert recommending that customers configure their FortiGate units to block traffic on UDP port 8998.

Joe Wells, chief antivirus architect at Fortinet and founder of the WildList Organization remarked: “This current SoBig strain is among the fastest spreading mass-mail attacks we’ve seen. We were successful in developing an antivirus response to block the spread

of the worm shortly after it was released. However, this particular threat has ‘time release’ elements that lie dormant and then activate automatically on infected systems. We urge customers to ensure that their FortiGate systems are configured to accept ‘push’ updates so that they receive protection with minimal delays. We also strongly recommend that customers use the myriad capabilities of their FortiGate systems – including the firewall subsystem – to block additional traffic that could be used to sustain the attack.”

The updates of antivirus and intrusion attack detection databases are delivered from the global FortiResponse™ Distribution Network, which ensures that FortiGate units worldwide are updated in real time in response to new attacks, and are able to detect and prevent threats from entering customer networks, without waiting for the unit or an administrator to request an update.

For more information on SoBig and other content security threats, visit the FortiResponse portal at <http://www.fortinet.com/FortiResponseCenter> and subscribe to Fortinet’s daily email newsletter alert to the latest virus, worm, intrusion and related malicious code threats to enterprise and service provider networks.

About Fortinet (www.fortinet.com)

Fortinet's award-winning FortiGate series of ASIC-accelerated antivirus firewalls are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time – without degrading network performance. The FortiGate systems deliver a full range of network-level services – firewall, VPN, intrusion detection and traffic shaping – as well as application-level services such as antivirus and content filtering, in dedicated, easily managed platforms. Fortinet is privately held and based in Santa Clara, California.

