Latest Fortinet Threat Landscape Research Shows Re-Emergence of Torpig Botnet

Report Also Shows Steady Use of Spam IPs Despite Overall Reduction in Spam

SUNNYVALE, CA -- (MARKET WIRE) -- 04/13/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its latest 30-day Threat Landscape research, which showed the re-emergence of the Torpig botnet, accounting for 30 percent of new botnet activity. Most command and control detections for Torpig originated from machines in Russia and Sudan. By comparison, the Hiloti botnet accounted for roughly 15 percent of new botnet traffic -- the majority of which was found in Australia and Sweden.

"The rigid Torpig botnet has been around for years and typically spreads through infected Web pages installed with a rootkit (mebroot) that infects a system right from the master boot record," said Derek Manky, senior security strategist at Fortinet. "Since this compromises the chain of trust from the get-go, mebroot has the ability to bypass personal firewalls through the operating system. Gateway security can mitigate this threat by blocking mebroot related traffic."

Spam Activity
Spam rates continue to remain lower than average at about 30 percent following the takedown of the Rustock botnet in March. While rates remain low, the number of spamming IPs (machines) has not taken a large drop. Most spamming IP addresses observed were geolocated to machines in the U.S., India and Brazil.

"Oftentimes machines are infected with multiple viruses or botnets that can continue to send spam and siphon data, despite one threat being mitigated," Manky said.

About FortiGuard Labs
FortiGuard Labs compiled threat statistics and trends for the last four weeks based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against this vulnerability with the appropriate configuration parameters in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate®, FortiMail™ and FortiClient™ products.

The most recent Threat Landscape research, which includes the top threat rankings in several categories and specific regions, is available now. Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog and Fortinet's monthly Security Minute videocast.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Media Contact:

Jennifer Leggio

Fortinet, Inc.

+1-408-486-7876

jleggio@fortinet.com

Source: Fortinet

News Provided by Acquire Media